U.S. Customs and
Border Protection

Office of Technology Innovation and Acquisition (OTIA)

Secure Border Initiative Network (SBI*net*) Block 1 ((b) (7)(E)) Capabilities and Limitations

Version 2.0– Post–Deployment Assessment
Draft
October 2011

~~This document was~~ prepared for authorized distribution only. Information contained ~~herein is~~ exempt from public disclosure under ~~United States Code~~ (USC) subsection (b), 5 USC 552. It ~~has not been~~ approved for public release.

~~**For Official Use Only**~~

Version	Date	Description
V1.0	10/15/2010	Initial submission for the OTRR – Pre–operational testing capabilities and limitations.
D.1	09/29/2011	Secure Border Initiative Network (SBI*net*) Block 1 (b) (7)(E) Capabilities and Limitation - Post–deployment of the (b) (7)(E) SBI*net* *Block 1* System – testing capabilities and limitations.
D.2	10/31/2011	Secure Border Initiative Network (SBI*net*) Block 1 ((b) (7)(E) Capabilities and Limitation - Post–deployment of the (b) (7)(E) SBI*net* *Block 1* System – testing capabilities and limitations.

SBI*net* Block 1 ((b) (7)(E) [redacted]) Capabilities and Limitations

Table of Contents

List of Figures

List of Tables

SBI*net* Block 1 (b) (7)(E) Capabilities and Limitations

Executive Summary

In 2005, the Department of Homeland Security established the Secure Border Initiative (SBI) to help secure America's borders. Under this initiative, SBI*net* was established to provide surveillance, detection, command, control, and intelligence tools within a networked communication infrastructure to improve situational awareness and facilitate interdiction decisions along the Southwest Border (SWB). The initial deployment of SBI*net* capabilities, referred to as SBI*net* Block 1, was in the U.S. Border Patrol (USBP) Tucson Sector in the (b) (7)(E) and the (b) (7)(E) areas of responsibility (AOR). This document is an assessment of the capabilities and limitations (C&L) of the SBI*net* Block 1 system currently deployed in the (b) (7)(E).

This document is intended for the various stakeholders of the SBI*net* Block 1 system, which include USBP strategic leadership, station and sector level decision makers, and USBP agents/operators. To address these various stakeholder needs, this document describes the capabilities and limitations of the Block 1 system with respect to foundational operational capabilities (FOC), the USBP mission (as stated in the Concept of Operations), and basic operational functions of the system. Qualitative analyses were performed to assess the capabilities and limitations of the integrated system, as well as for the individual system components.

The SBI*net* Block 1 system consists of a series of (b) (7)(E) that are used to detect incursions at the border, and are operationally integrated into a computer system referred to as the common operational picture (COP). The COP displays (b) (7)(E) information, provides control of the (b) (7)(E) systems, records critical information, and allows monitoring of border activities in the resolution of potential threats and respond to incursions. The Block 1 system components addressed within this C&L document include the (b) (7)(E), (b) (7)(E) provide the infrastructure (b) (7)(E) (b) (7)(E) (b) (7)(E)

Overall, this assessment indicates that deployment of the (b) (7)(E) systems has enhanced USBP capabilities in conducting their mission. The current deployment of the SBI*net* Block 1 system has enhanced USBP's ability to deter illegal entry into the United States by increasing the probability of detection and apprehension within the stations in which they are deployed. The SBI*net* Block 1 system improves situational awareness and facilitates interdiction decisions along the SWB through the use of surveillance, detection, command, control, and (b) (7)(E) tools within a networked communication infrastructure. It has added capabilities and resources that the USBP agents utilize on a daily basis for conducting their mission. A key limitation of the system is (b) (7)(E) (b) (7)(E) In addition, components of the Block 1 system (b) (7)(E)

The most significant capabilities and limitations are listed below:

Capabilities:

- Strategic Level
  - (b) (7)(E)
  -
- Mission Level
  - (b) (7)(E)
  -
  -
  -
  -
- Operational Functions
  - (b) (7)(E)
  -
  -

Limitations:

- Strategic Level
  - (b) (7)(E)
  -
- Mission Level
  - (b) (7)(E)

  - (b) (7)(E)

- Operational Functions
  - (b) (7)(E)

The document lists the capabilities and limitations based on the FOC, USBP mission elements, and operational functions. In addition, this document contains operational 2-dimensional LOS viewsheds for both AORs and user Quick Reference Guides (QRG) to assist the agents in their day-to-day operations. The QRGs consolidate workarounds utilized to address system limitations, training materials, and hints from experienced agents ("super users").

This Page Intentionally Blank

1. INTRODUCTION

In 2005, the Department of Homeland Security established the Secure Border Initiative (SBI) to help secure America's borders. Under this initiative, SBI*net* was established to provide surveillance, detection, command, control, and intelligence tools within a networked communication infrastructure to improve situational awareness and facilitate interdiction decisions along the Southwest Border (SWB). The initial deployment of SBI*net* capabilities, referred to as SBI*net* Block 1, took place in the Customs and Border Protection (CBP) Border Patrol (BP) Tucson Sector. Within the Tucson sector, the Block 1 system was deployed in areas of responsibility (AORs) for the (b) (7)(E), referred to as the (b) (7)(E) deployments, respectively. This document is an assessment of the capabilities and limitations (C&L) of the deployment of the SBI*net* Block 1 system.

This document is intended for various stakeholders of the SBI*net* Block 1 system, which include agent operators, strategic leadership, and other personnel supporting SBI activities. This document provides a qualitative assessment of the SBI*net* Block 1 system's capabilities and limitations with respect to USBP foundational operational capabilities (FOCs)[1], the USBP mission, and basic operational functions of the system.

1.1 BACKGROUND

The purpose of the SBI*net* Block 1 system is to provide a capability that supports the interdiction of illegal immigration and other border crossing threats. These threats include Alien Smuggling Organizations, Drug Trafficking Organizations, terrorist activities, and weapons shipments. Illegal incursions at the border occur through a variety of means. The threat is mobile and adaptive. SBI*net* provides some level of capability to detect entries (items of interest) (b) (7)(E) (b) (7)(E) and facilitate an effective and efficient response to the entry, enabling appropriate law enforcement resolution.

The initial deployment of the SBI*net* Block 1 system was in the CBP Tucson Sector. The sector is divided into eight station AORs. This document is an assessment of the C&L of the SBI*net* Block 1 system deployed in the (b) (7)(E), referred to as (b) (7)(E) respectively.

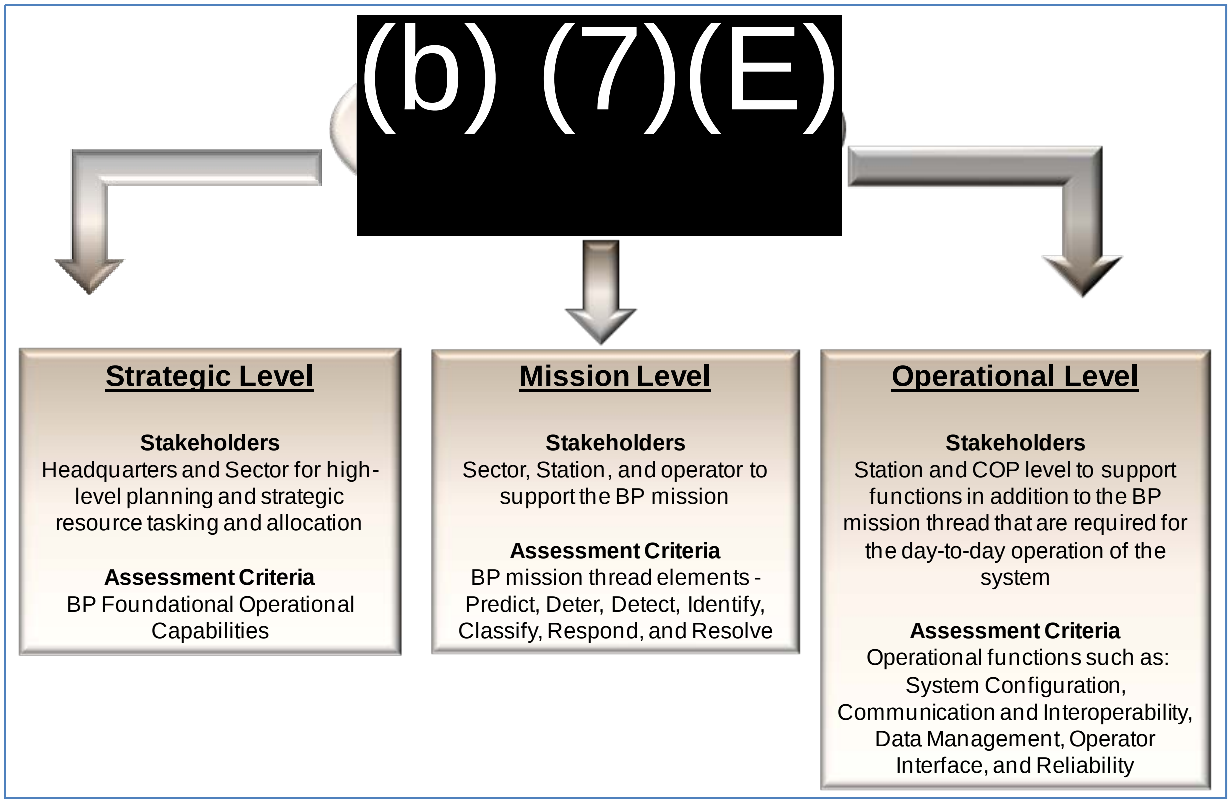
The Block 1 system was intended to address the needs of various stakeholders and provide information for different levels of support (Figure 1–1). Therefore, this qualitative assessment of the C&L was conducted at three levels:

- **Strategic** – At the strategic level for stakeholders, such as the USBP headquarters, the document is intended to provide input for high-level planning, concept of operations (CONOPS) development, and strategic resource tasking and allocation. As such, the C&L were assessed with respect to the USBP FOCs. (Appendix A)

[1] Email communication from USBP, June 17, 2011, Definitions – Measures of Impact (MOIs).

- **Mission –** At the sector and station level, the document is intended to support the overall BP mission; therefore, the C&L were assessed with respect to the USBP mission elements (predict, deter, detect, identify, classify, respond, and resolve).
- **Operational –** At the station level, for the agents using and maintaining the system on a day-to-day basis. This includes an assessment of the operational functions that support/facilitate the USBP mission elements such as system configuration, communication and interoperability, data management, operator interface, reliability, etc.,

These assessments were conducted both at the system level (for high-level planning, resource allocation, etc.) and at a component level (for use by the system operator to assist in day-to-day operations).



Strategic Level

Stakeholders
Headquarters and Sector for high-level planning and strategic resource tasking and allocation

Assessment Criteria
BP Foundational Operational Capabilities

Mission Level

Stakeholders
Sector, Station, and operator to support the BP mission

Assessment Criteria
BP mission thread elements - Predict, Deter, Detect, Identify, Classify, Respond, and Resolve

Operational Level

Stakeholders
Station and COP level to support functions in addition to the BP mission thread that are required for the day-to-day operation of the system

Assessment Criteria
Operational functions such as: System Configuration, Communication and Interoperability, Data Management, Operator Interface, and Reliability

(b) (7)(E)

Figure 1–1: Block 1 Capabilities and Limitation Document Intended Stakeholders and Assessment Criteria

The development of the Block 1 C&L report was tightly coupled with two other CBP references: the CONOPS for system usage (Reference [1]) and the system training document (Reference [2]). The CONOPS and the SBI*net* Block 1 training manual are used and referenced throughout this document to define the mission space and associated terms, definitions, and functionality. Figure 1–2 depicts a notional representation of the complementary content provided by these documents and their related activities.

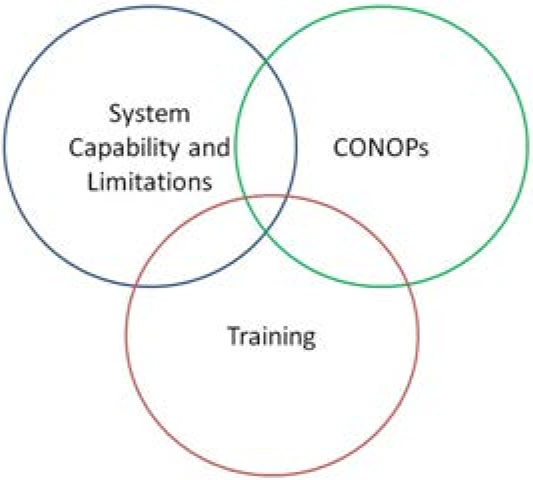


Figure 1–2: Complementary and Shared Content of System Information for Operator Use

Specifically, each of these reports provides the following to the operators:

- *Capabilities and Limitations (C&Ls)* – The C&L document to provides the operational end-user an understanding of the capabilities and limitations of the system. This promotes a more thorough understanding by the user of what the system can and cannot do. It provides the operator inherent system limitations and capabilities.
- *SBInet CBP Concept of Operations (CONOPS)* – The system CONOPS provides a description and rationale of the system functional capabilities, from the operator's point of view. It summarizes the needs goals and characteristics of the system's user community including operators, maintainers, and support personnel. It defines any critical, top-level performance requirements or objectives stated either qualitatively or quantitatively, with system rationale. The CONOPS document should contain the roles and responsibilities and the set of skills needed for operations and maintenance of the system.
- *System Training* – Training has the goal of teaching the operator how to use the system.. Effective training begins with a thorough understanding of the CONOPS and the C&L of the system. Updates to training content uses feedback from trainees after they have operational experience on the system.

While each of these elements provides a unique view of the Block 1 system, together they provide the operators with a better understanding and increased knowledge of the system to improve system proficiency and mission success.

1.2 PURPOSE

For both the strategic and mission levels, the purpose of this document is to:

- Document capabilities and limitations of the Block 1 system with respect to the FOCs and the mission elements.
- Convey technical information for CONOPS development.

At a tactical level, the purpose of the SBI*net* Block 1 C&L assessment report is to:

- Document capabilities and limitations of the Block 1 system with respect to operational functions.
- Provide the operator an operational understanding of the Block 1 components.
- Facilitate learning, acclimation, and operational use of the system by operators.

1.3 SCOPE

The SBI*net* Block 1 C&L assessment addresses the configuration of the (b) (7)(E) system. It addresses the C&L of the overall Block 1 system as well as the following system components:

(b) (7)(E)

- Common Operational Picture (COP)

Legacy equipment and resources being utilized in conjunction with the Block 1 deployment are not included in the scope of this document. However, the interaction/architecture in relation to the Block 1 system with the following components is further explained in Section 2:

(b) (7)(E)

1.4 METHODOLOGY

The following approach was used to assess the capabilities and limitations of the SBI*net* Block 1 system and document the system components, functions, and perceived gaps.

- Reviewed CBP provided documentation. Key documents reviewed and cited are listed in Section 8. Additional documentation for the SBI*net* system was received through the Program Information Management System, a database of resources managed by CBP. Data collected during system acceptance testing (SAT), Reference [3], and the operational testing was reviewed and used where applicable. Threat track data was not available to evaluate Block 1 system performance within the system viewsheds.
- Conducted in-depth review of the major components of the system.
- Conducted workshops (onsite and teleconferences) with [redacted] Border Patrol agents. During these workshops, agents provided feedback regarding SBI*net* Block 1 system C&Ls, as well as suggestions for information format and content.
- Assessed—based on subject matter expert (SME) input and direct feedback from operators—the degree to which the [redacted] systems help CBP meet its operational objectives. The assessment was conducted at a system level and at the component ([redacted] and COP) level. The terms used are qualitative in nature and represent the opinions of the component SMEs.

Table 1–1 depicts the legend and describes the qualitative descriptors used in the assessment for the system and component-level capabilities and limitations. To provide flexibility to the C&L document stakeholders, the C&Ls are listed at both the system and component level.

Table 1–1: Block 1 USBP Strategic Planning, Mission Elements, and Tactical Functions Rankings

System and Subcomponent
🟩 **Significant** Provides a considerable portion of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.
🟨 **Limited** Provides some portion of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.
🟧 **Minimal** Provides basic elements of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.
🟥 **None**

The SBI*net* Block 1 system and component C&Ls are listed in tabular form with respect to the USBP FOCs, the USBP mission, and basic operational functions of the system. The tables contain subcategories of operational functions where applicable. Definitions of the USBP FOCs, mission elements, and operational functions are provided in Appendix A.

1.5 SBI*NET* BLOCK 1 CAPABILITIES AND LIMITATIONS DOCUMENT OVERVIEW

This document details the Block 1 C&L with respect to the USBP mission and conveys this information in a manner that supports associated analysis functions for various stakeholders ranging from strategic to tactical levels. No single document can meet all preferred organizational formats for intended users; therefore, a logical approach (from a strategic/system level down to component/tactical level) was adopted. This document provides the following information:

- Overview of SBI*net* Block 1 system, system architecture, and description (Section 2).
- C&Ls at the system level with respect to mission FOCs, mission elements, and operational functions (Section 3).
- C&Ls by system components with respect to mission FOCs, mission elements, and operational functions (Section 4).
- Summary (Section 5)
- References (Section 6), Glossary (Section 7), and Acronyms and Abbreviations (Section 8)
- Additional Documents (Section 9)
- Definitions of USBP Foundational Operational Capabilities, Mission Elements, and Operational Functions (Appendix A)
- System viewsheds ((b) (7)(E) without environmental impacts) (Appendix B)
- Capability Vignettes based on Capability Vignettes developed in the Secure Border Initiative Integrated Concept of Operations (CONOPS) and Requirements Specification (Appendix C)
- System Component Functional and Physical Descriptions: (b) (7)(E)(Appendix D), Communications (Appendix E),(b) (7)(E)(Appendix F),(b) (7)(E)(Appendix G), and COP (Appendix H).
- Open Architecture Principles (Appendix I)
- Quick Reference Guides (Appendix J)

References and links (internal and external) are provided throughout the remaining sections of the document. To be effective, this document (in electronic form) must reside at the root level of the file structure with the references included in a folder.

2. BLOCK 1 SYSTEM ((b) (7)(E))

The Block 1 system deployed in (b) (7)(E) are quite similar, and for the purposes of an overview description, will be treated as the same, expect where identifying unique differences is required (e.g. viewsheds depictions, etc.). The following sections provide a system overview, the system architecture, and description of the *SBInet* Block 1 system.

2.1 BLOCK 1 SYSTEM OVERVIEW

The SBI*net* Block 1 system is a technology solution implemented to provide USBP agents with 24/7 visibility and surveillance, and Command, Control, Communications, Coordination, and Intelligence (C4I) capabilities. The system consists of a network (b) (7)(E), (b) (7)(E) and other situational awareness information integrated into a COP monitored at the individual stations.

The sensor components for the Block 1 system are the (b) (7)(E) (b) (7)(E) (b) (7)(E) that houses the COP. (b) (7)(E)

Functionally, the (b) (7)(E) provide broad coverage for the AOR. The radar (b) (7)(E)

2.2 BLOCK 1 SYSTEM DESCRIPTION AND ARCHITECTURE

Operators use multiple CBP assets, including the Block 1 system, to provide situational awareness. In addition, the Block 1 COP operators have many of these CBP assets available to them in forming their picture of situational awareness. Figure 2–1 is a high-level system interface diagram that shows (b) (7)(E) Block 1 components are indicated in dark blue, legacy equipment partially integrated is in grey/light blue, and the equipment/sensors not integrated are in grey.

(b) (7)(E)

Figure 2–1: SBI*net* High-Level System and Interfaces

(b) (7)(E) Details (b) (7)(E) are provided in Appendix E.

The data from the sensors that are not integrated into the COP display are available to the agents via a number of other means (b) (7)(E). It should be noted that:

- (b) (7)(E) The (b) (7)(E) were not operational and the performance of the (b) (7)(E) is not discussed in this document (indicated in light blue in the figure).
- (b) (7)(E)
- The software components and features of the [redacted] are also outside the scope of this document.

Each AOR has both (b) (7)(E) The (b) (7)(E) include an (b) (7)(E). Details for these individual components can be found in Section 4.2. Because of terrain and long distances required between the locations of the (b) (7)(E), additional (b) (7)(E) are required to act as relays for (b) (7)(E) data and information. (b) (7)(E) are deployed manually by agents in the field (b) (7)(E) (b) (7)(E) (see Section 4.4 for additional details).

(b) (7)(E).

The SBI*net* system has been deployed in the CBP Tucson Sector in the (b) (7)(E) and (b) (7)(E) Data sharing (within the two stations, USBP, and with partner agencies) is not implemented as intended. The (b) (7)(E) system work independently and do not share a COP. Figure 2–2 depicts the entire Tucson Sector and its eight Stations. (b) (7)(E) includes (b) (7)(E) miles of the international border between the United States and Mexico surrounding the (b) (7)(E) Arizona, port of entry (POE). (b) (7)(E) AOR includes (b) (7)(E) miles of international border. Viewsheds of individual towers in the (b) (7)(E) Stations are provided in Appendix A.

(b) (7)(E)

Figure 2–2: Tucson Sector Station AOR Boundaries

3. BLOCK 1 SYSTEM CAPABILITIES AND LIMITATIONS

he purpose of the SBI*net* Block 1 system is to provide a capability that supports the interdiction of illegal immigration and other border-crossing threats. At the strategic level (for stakeholders such as the USBP headquarters), this document is intended to provide input for high-level planning, CONOPS development, and strategic resource tasking and allocation. Therefore, the C&Ls of the Block 1 system were assessed with respect to the FOCs, USBP mission elements, and operational functions, each detailed in the sections that follow.

Within each section, the C&L are provided in tabular form that, where applicable, contain subcategories of operational functions (listed in Appendix A).

3.1 FOUNDATIONAL OPERATIONAL CAPABILITIES

The USBP FOCs represent those elements necessary to effectively execute the mission of protecting and securing the borders of the United States outside of the POEs. The USBP definitions of the Generation 3 Analysis of Alternatives FOCs (also referred to as Measures of Impact) are provided in Appendix A. In general, these FOCs characterize USBP capabilities in terms:

- **Impedance and Denial**
- **Operational Access, Mobility and Rapid Response.** Due to the nature of this FOC and for the purposes of this document, "operational access" (for example, roads, transportation systems, agreements) is assessed separately from "mobility and rapid response" (for example, enhanced security, enhanced operations)
- **Visibility and Surveillance**
- **Command, Control, Communications, Coordination, and Intelligence (C4I)**
- **Security Partnership**

At the strategic/highest level, the SBI*net* C&Ls are evaluated with respect to these FOCs. This assessment was conducted at a system level since individually the components ((b) (7)(E) (b) (7)(E), and COP) contribute minimally at the evaluation level of the FOCs (e.g., (b) (7)(E) However, as a system, they can contribute to BP FOCs.

The deployment of the SBI*net* Block 1 system has enhanced BP's ability to deter illegal entry into the United States by increasing the probability of detection and apprehension within the (b) (7)(E) AORs. In addition, **the Block 1 system enhances the capability to detect, identify targets, and classify (aid in determining the level of threat).** The system provides visual information that enables faster response and enhances agent safety. The system nominally provides BP agents with 24 hours a day, 7 days a week target detection capability along portions of border using (b) (7)(E) sensor modalities. (b) (7)(E)

(b) (7)(E)

The Block 1 system is intended to use (b) (7)(E) .

The Block 1 system uses (b) (7)(E)

Table 3–1 details the capabilities and limitations of the (b) (7)(E) system when assessed/mapped against the FOCs. As previously noted, the assessment terms are qualitative in nature and are based on component SMEs, CBP, and USBP operator inputs. Overall, the assessment indicates that deployment of the (b) (7)(E) system is an enhancement of the USBP FOCs.

Table 3–1: Block 1 System Capabilities and Limitations with Respect to the USBP FOCs

FOC	Capability	Limitation
(b) (7)(E)	(b) (7)(E)	

FOC	Capability	Limitation
(b) (7)(E)	(b) (7)(E)	
(b) (7)(E)		

3.2 MISSION ELEMENTS

One of CBP's strategic objectives is to establish and maintain effective control of air, land, and maritime borders with the appropriate mix of infrastructure, technology, and personnel. Objective 1.1 in *CBP's 2009–2014 Strategic Plan*[2] states that CBP must:

> *"Establish and maintain effective control of air, land, and maritime borders through the use of the appropriate mix of infrastructure, technology and personnel. A segment of the border between ports of entry is considered under effective control when CBP can simultaneously and consistently achieve the following: (1) **detect** illegal entries into the United States; (2) **identify** and **classify** these entries to determine the level of threat involved; (3) efficiently and effectively **respond** to these entries; and (4) bring each event to a satisfactory law enforcement **resolution**."*

The SBI*net* CONOPS lists the following mission elements (key mission elements are defined in Appendix A):

- **Predict**
- **Deter**
- **Detect**
- **Indentify/Classify**
- **Track**
- **Respond**
- **Resolve**

The mission elements are structured as a series of activities. A typical mission element could be described as the COP operator being alerted to a potential target based on (b) (7)(E) information (b) (7)(E) The COP operator can then (b) (7)(E)

At an overall mission level perspective, the SBI*net* system is **effective in supporting the mission elements**. (b) (7)(E)

[2] (b) (7)(E)

(b) (7)(E)

Table 3–2 details the capability and limitation assessment with respect to the mission elements at a system level (for component-level details, see Section 4). The terms used are qualitative in nature and represent the opinions of the component SMEs, CBP, and USBP operator inputs.

Table 3–2: Block 1 System Capabilities and Limitations with Respect to USBP Mission

Block 1 System Mission Elements		
Element	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

Block 1 System Mission Elements		
Element	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

Block 1 System Mission Elements		
Element	**Capability**	**Limitation**
(b) (7)(E) [redacted]	(b) (7)(E) [redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Along with the mission elements defined by USBP, capability vignettes generated as a part of the SBI*net*, CONOPS were used to analyze the mission processes and workflow as it pertains to the capabilities and limitations of the SBI*net* system. As described in the CONOPS, the capability vignettes were intended for operational users, software architects, and trainers. Appendix C contains the C&L assessment with respect to the vignettes provided by CBP for the SBI*net* system.

3.3 OPERATIONAL FUNCTIONS

The system functional assessment addresses how the system facilitates operator use, which includes system reliability, system configuration, data management, maintenance, operator interface, etc. To accomplish this assessment, some basic operational functions and sub-functions were identified to characterize the user interface to the system (further detailed in Appendix A). The assessment of the Block 1 system against each of these functional categories and sub-categories is provided in the tables below. Note that each of these tables reflects the relative contribution of the capability or limitation, and the terms used are qualitative in nature and represent the opinions of the component SMEs, CBP, and USBP operator inputs.

- **Configuration** (configurable, information assurance, data security, etc.)
- **Communication and Interoperability** (receive/process raw data, send/receive data from agents or non-CBP assets, etc.)
- **Data Management** (fuse data, store data, agent safety, etc.)
- **Operator Interface** (user friendliness, filter data, display history, etc.)
- **Reliability, Maintainability, Availability** (reliable (b) (7)(E) operation, availability, etc.)

From a operational/tactical level perspective, the SBI*net* system provides the operators with a user friendly interface (b) (7)(E) The system stores and archives video data allowing for subsequent retrieval and resolution of incidents. The (b) (7)(E) used in Block 1 are compatible (b) (7)(E). The station utilizes a combination of on-the-job training (OJT), codified tactics, techniques, and procedures, and quick reference guides to aid in the efficient transfer of knowledge to new operators and reduce the time necessary to become proficient in system operation.

The capability and limitations with respect to the system functions was conducted at a system level and at the component ((b) (7)(E) and COP) level (Section 4). Table 3–3 through Table 3–7 detail the SBI*net* Block 1 system capabilities and limitations with respect to each of the five broad functional categories, and indicate the relative contribution of the capability or limitation. The terms used are qualitative in nature and represent the opinions of the component SMEs.

Table 3–3: Block 1 System Configuration Functions

Block 1 System Configuration Functions		
Function	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	
Information Assurance at Multiple Layers		
(b) (7)(E)		

Table 3–4: Block 1 System Communication and Interoperability Functions

Block 1 System Communication and Interoperability Functions		
Function	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	
(b) (7)(E)		

Block 1 System Communication and Interoperability Functions		
Function	Capability	Limitation
[redacted]	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	[redacted]	[redacted]
(b) (7)(E)	[redacted]	[redacted]

Table 3–5: Block 1 System Data Management Functions

Block 1 System Data Management Functions		
Function	Capability	Limitation
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	[redacted]	[redacted]

Block 1 System Data Management Functions		
Function	**Capability**	**Limitation**
🟩 (b) (7)(E)	(b) (7)(E)	
🟩		
🟨		
🟩		

Table 3–6: Block 1 System Operator Interface Functions

Block 1 System Operator Interface Functions		
Function	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	
r		
(b) (7)(E)		
(b) (7)(E)		

Block 1 System Operator Interface Functions		
Function	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

Table 3–7: Block 1 System Reliability, Maintainability, and Availability Functions

System Reliability, Maintainability, and Availability Functions		
Function	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	
(b) (7)(E)		
(b) (7)(E)		
(b) (7)(E)		

System Reliability, Maintainability, and Availability Functions		
Function	**Capability**	**Limitation**
Built–in Test/Alert for Failures/Degraded Performance	Insufficient data to determine	
Preventative Maintenance/Test	Insufficient data to determine	
Minor Repair within Non-technician Operator Capability	Insufficient data to determine	
Repair Times	Insufficient data to determine	

4. BLOCK 1 COMPONENTS CAPABILITIES AND LIMITATIONS

While the previous sections described the system characteristics, the capabilities and limitations of the system's components with respect to the USBP mission elements and operational functions are detailed in the following sections. At a component level, the capability and limitations tables provide the operator with an understanding of the technical operation of the system and facilitate efficient operator system learning, system acclimation, and operational use.

4.1 COMMON OPERATIONAL PICTURE

The COP provides an operational picture of portions of the AOR covered by (b) (7)(E). It enables detection, identification, and supports classification of entities through the integrated examination of (b) (7)(E) event data display. This section contains tables describing the capabilities and limitations of the COP. The first table (Table 4–1) describes the capabilities and limitations of Block 1 system COP with respect to the overall mission element functions.

Table 4–1: Block 1 System COP Mission Element Functions

COP Mission Element Functions		
Function	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

COP Mission Element Functions		
Function	**Capability**	**Limitation**
	(b) (7)(E) [redacted]	[redacted]
(b) (7)(E) [redacted]		

COP Mission Element Functions		
Function	**Capability**	**Limitation**
	(b) (7)(E)	
(b) (7)(E)		
(b) (7)(E)		

COP Mission Element Functions		
Function	**Capability**	**Limitation**
[redacted] (b) (7)(E)	[redacted] (b) (7)(E)	[redacted]

Table 4–2 summarizes an assessment of the COP configuration functions such as the options available for [redacted] (b) (7)(E).

Table 4–2: Block 1 System COP Configuration Functions

COP Configuration Functions		
Function	**Capability**	**Limitation**
[redacted] (b) (7)(E)	[redacted] (b) (7)(E)	[redacted]
Information Assurance at Multiple Layers		
[redacted] (b) (7)(E)		

The SBI*net* Block 1 system COP was intended to provide the capability for communications and interoperability between the COP, various system components, and other assets and resources. Table 4–3 summarizes an assessment of the capabilities and limitations of the COP communication and interoperability functions.

Table 4–3: Block 1 System COP Communications and Interoperability Functions

COP Communications and Interoperability Functions		
Function	**Capability**	**Limitation**
	(b) (7)(E)	
(b) (7)(E)		
(b) (7)(E)		

COP Communications and Interoperability Functions		
Function	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

The intent of the SBI*net* Block 1 system was to obtain and fuse data from various system components and operational resources to display on the COP. Table 4–4 summarizes an assessment of the capabilities and limitations of the COP data management functions.

Table 4–4: Block 1 System COP Data Management Functions

COP Data Management Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

COP Data Management Functions		
Functions	**Capability**	**Limitation**
	(b) (7)(E) [redacted]	[redacted]
(b) (7)(E) [redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

From an interface perspective, the COP was assessed in terms of its ability to provide functional controls that support operational goals. Table 4–5 summarizes these interface functions and assesses the capabilities and limitations inherent in each function.

Table 4–5: Block 1 System COP Operator Interface Functions

COP Operator Interface Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

COP Operator Interface Functions		
Functions	**Capability**	**Limitation**
	(b) (7)(E) [redacted]	[redacted]
	[redacted]	[redacted]
(b) (7)(E) [redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

COP Operator Interface Functions		
Functions	**Capability**	**Limitation**
	(b) (7)(E)	
(b) (7)(E)		

COP Operator Interface Functions		
Functions	**Capability**	**Limitation**
	(b) (7)(E)	

In addition to system interfaces, the COP was assessed in terms of its reliability, maintainability, and availability. Table 4–6 summarizes these functions and assesses the capabilities and limitations inherent in each function.

Table 4–6: Block 1 System COP Reliability, Maintainability, and Availability Functions

COP Reliability, Maintainability, and Availability (RMA) Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

COP Reliability, Maintainability, and Availability (RMA) Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	[redacted]	[redacted]
(b) (7)(E)	[redacted]	[redacted]
Preventative Maintenance/Test	[redacted]	[redacted]
Minor Repair within Non-technician Operator Capability	[redacted]	[redacted]
Repair Times	[redacted]	[redacted]

4.2 [redacted]

The [redacted] for the SBI*net* Block 1 system is intended to help operators detect and resolve targets and provide USBP Agents with information pertaining to the location of targets, agents, and moving vehicles. This section contains a number of tables describing the capabilities and limitations of the Block 1 [redacted] system from a functional perspective. The first table (Table 4–7) describes the capabilities and limitations of the [redacted] system with respect to the overall mission element functions.

Table 4–7: Block 1 System Radar Mission Element Functions

[redacted] Mission Element Functions		
Functions	**Capability**	**Limitation**
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]		

<table>
<tr><th colspan="3">(b) (7)(E) Mission Element Functions</th></tr>
<tr><th>Functions</th><th>Capability</th><th>Limitation</th></tr>
<tr><td>(b) (7)(E)</td><td colspan="2">(b) (7)(E)</td></tr>
</table>

(b) (7)(E) Mission Element Functions		
Functions	**Capability**	**Limitation**
	(b) (7)(E)	
(b) (7)(E)		

Table 4–8 summarizes the configuration capabilities and limitations of the (b) (7)(E). Some functionality of the (b) (7)(E) can be configured by the operator or system administrator; the rest must be conducted by the vendor.

Table 4–8: Block 1 System (b) (7)(E) Configuration Functions

(b) (7)(E) Configuration Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

(b) (7)(E) Configuration Functions		
Functions	**Capability**	**Limitation**
	(b) (7)(E)	
Information Assurance at Multiple Layers	Insufficient data to determine	Insufficient data to determine
Data Security	Insufficient data to determine	Insufficient data to determine

From an interoperability and communications standpoint, the (b) (7)(E) component provides the Block 1 system with raw (b) (7)(E) data. Table 4–9 summarizes these functions and assesses the capabilities and limitations inherent in each function.

Table 4–9: Block 1 System (b) (7)(E) Communication and Interoperability Functions

(b) (7)(E) Communication and Interoperability		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	[redacted]

In addition to providing raw data, the (b) (7)(E) can also be assessed in terms of its ability to create, identify, and classify tracks. In Table 4–10, the (b) (7)(E) functions are summarized and assessed in light of their capabilities and limitations.

Table 4–10: Block 1 System (b) (7)(E) Functions

(b) (7)(E) Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	[redacted]

(b) (7)(E) Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

In Table 4–11, the (b) (7)(E) capabilities and limitations for data management functions are assessed.

Table 4–11: Block 1 System(b) (7)(E) Data Management Functions

(b) (7)(E) Data Management Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

(b) (7)(E) Data Management Functions		
Functions	Capability	Limitation
	(b) (7)(E)	
(b) (7)(E)		

(b) (7)(E) Data Management Functions		
Functions	Capability	Limitation
(b) (7)(E)	(b) (7)(E)	

The (b) (7)(E) can also be assessed in terms of its reliability, maintainability, and availability. Table 4–12 summarizes these functions and assesses the capabilities and limitations inherent in each function.

Table 4–12: Block 1 System (b) (7)(E) Reliability, Maintainability, and Availability Functions

(b) (7)(E) Reliability, Maintainability, and Availability (RMA)		
Functions	Capability	Limitation
(b) (7)(E)	(b) (7)(E)	

(b) (7)(E) Reliability, Maintainability, and Availability (RMA)		
Functions	**Capability**	**Limitation**
	(b) (7)(E)	
(b) (7)(E)		
Preventative		
(b) (7)(E)		
Repair Times		

4.3 (b) (7)(E)

The (b) (7)(E) used for the SBI*net* Block 1 system is made of (b) (7)(E) components. It is intended to provide operators with (b) (7)(E) displays to help identify, classify, respond, and resolve targets. In addition, the (b) (7)(E) used for determining target locations, is considered as part of the (b) (7)(E) This section contains a number of tables describing the capabilities and limitations of the Block 1 (b) (7)(E) from a functional perspective. For Tables 4–13 through 4–18, an additional column is provided to indicate for which system component (b) (7)(E) the capability or limitation applies.

The first table (Table 4–13) describes the capabilities and limitations of the (b) (7)(E) with respect to the overall mission thread functions.

Table 4–13: Block 1 System (b) (7)(E) Mission Element Functions

(b) (7)(E) Mission Elements Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)		
🟩			

(b) (7)(E) Mission Elements Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)		
(b) (7)(E)			

(b) (7)(E) Mission Elements Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)		

Some functionality of the (b) (7)(E) can be configured by the operator. Table 4–14 summarizes the configuration capabilities and limitations of the (b) (7)(E)

Table 4–14: Block 1 System (b) (7)(E) Configuration Functions

(b) (7)(E) Configuration Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)		
Information Assurance at Multiple Layers			
(b) (7)(E)			

The SBI*net* Block 1 system provides the capability for communications and interoperability between the COP, various system components, and other assets and resources. Table 4–15

[3] Feature may not be available. It is shown in CBP "Lesson 1.2: COP Monitor – Instructor Guide," June 2010, but not included in training material Lesson 2.3 of COP Training Material Presentation (12–OP_Mod_2_Lesson_2.3_PTT_Final_30June2010.ppt).

summarizes these functions and assesses the capabilities and limitations inherent in each function with a specific focus on the (b) (7)(E)

Table 4–15: Block 1 System (b) (7)(E) Communication and Interoperability Functions

(b) (7)(E) Communication and Interoperability Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)		

(b) (7)(E) Communication and Interoperability Functions			
Functions	(b) (7)(E)	Capability	Limitation
		(b) (7)(E)	

Data from various system components and operational resources are fused together by the SBI*net* Block 1 system and displayed on the COP. In Table 4–16, various data management functions related to the (b) (7)(E) are assessed.

Table 4–16: Block 1 System (b) (7)(E) Data Management Functions

(b) (7)(E) Data Management Functions			
Functions	Camera	Capability	Limitation
(b) (7)(E)	(b) (7)(E)		

From an interface perspective, the (b) (7)(E) can be assessed in terms of its operator interface functions. Table 4–17 summarizes these interface functions and assesses the capabilities and limitations inherent in each function.

Table 4–17: Block 1 System (b) (7)(E) Operator Interface Functions

(b) (7)(E) Operator Interface Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)		

(b) (7)(E) Operator Interface Functions			
Functions	(b) (7)(E)	Capability	Limitation
🟩	(b) (7)(E)		
(b) (7)(E)			

The(b) (7)(E)system can also be assessed in terms of its reliability, maintainability, and availability. Table 4–18 summarizes these functions and assesses the capabilities and limitations inherent in each function.

Table 4–18: Block 1 System(b) (7)(E)Reliability, Maintainability, and Availability Functions

(b) (7)(E) Reliability, Maintainability, and Availability (RMA) Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)		

(b) (7)(E) Reliability, Maintainability, and Availability (RMA) Functions			
Functions	(b) (7)(E)	**Capability**	**Limitation**
	(b) (7)(E)		
(b) (7)(E)			
Preventative Maintenance/ Test			
Minor Repair within Non-technician Operator Capability			
Repair Times			

4.4 (b) (7)(E)

(b) (7)(E). The (b) (7)(E) (part of the Block 1 deployment) were not operational in (b) (7)(E). Therefore, performance of the (b) (7)(E) is not discussed in this document, however the fact that these are not currently available to the operational elements are considered as a limitation, and marked as such.

From an interface perspective, the (b) (7)(E) system is not integrated with the Block 1 COP. The operator can view the (b) (7)(E) location on the COP display. All (b) (7)(E) alerts are received via the (b) (7)(E) (b) (7)(E)

The COP receives (b) (7)(E).[4] (b) (7)(E) This section contains a number of tables describing the capabilities and limitations of the integration and use of the deployed (b) (7)(E) from a functional perspective. Table 4–19 describes the capabilities and limitations of the (b) (7)(E) system with respect to the overall mission element functions.

Table 4–19: Block 1 System (b) (7)(E) Mission Elements Functions

(b) (7)(E) Mission Elements Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

[4] (b) (7)(E), Secure Border Initiative SBInet Program, Interface Control Document, February 23, 2010.

(b) (7)(E) Mission Elements Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

Table 4–20 summarizes the configuration capabilities and limitations of the (b) (7)(E).

Table 4–20: Block 1 System (b) (7)(E) Configuration Functions

(b) (7)(E) Configuration Function		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

The SBI*net* Block 1 system provides the capability for communications and interoperability between the COP, various system components, and other assets and resources. Table 4–21 summarizes these functions and assesses the capabilities and limitations inherent in each function with a specific focus on the (b) (7)(E).

Table 4–21: Block 1 System (b) (7)(E) Communication and Interoperability Functions

(b) (7)(E) Communication and Interoperability Functions		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

Table 4–22 summarizes the Data Management capabilities and limitations of the (b) (7)(E).

Table 4–22: Block 1 System (b) (7)(E) Data Management Functions

Data Management Function		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

The (b) (7)(E) can also be assessed in terms of its reliability, maintainability, and availability. Table 4–23 summarizes these functions and assesses the capabilities and limitations inherent in each function.

Table 4–23: Block 1 System (b) (7)(E) Reliability, Maintainability, and Availability Functions

Reliability, Maintainability, and Availability (RMA) Function		
Functions	**Capability**	**Limitation**
(b) (7)(E)	(b) (7)(E)	

5. SUMMARY

The purpose of the SBI*net* Block 1 system was to provide a capability that supports the interdiction of illegal immigration and other border-crossing threats. The current deployment of the SBI*net* Block 1 system has enhanced USBP's ability to deter illegal entry into the United States by increasing the probability of detection and apprehension (b) (7)(E) (b) (7)(E). The SBI*net* Block 1 system improves situational awareness and facilitates interdiction decisions along the SWB through the use of surveillance, detection, command, control, and (b) (7)(E) tools within a networked communication infrastructure. It has added capabilities and resources that the USBP agents utilize on a daily basis for conducting their mission.

Capabilities for the agents provide the following:

(b) (7)(E)

A key limitation of the system is that (b) (7)(E). Some components of the Block 1 system were not implemented as intended, such as:

(b) (7)(E)

Subsequent deployment of this system or subsequent systems should consider these gaps. There are planned upgrades (spring/summer 2012) to the system to address some of the limitations of the individual components. Upgrades will provide the agents with greater control over the system components (specifically the (b) (7)(E)) and with additional (b) (7)(E).

This Page Intentionally Blank

6. REFERENCES

[1] U.S. Department of Homeland Security, "Draft CBP Concept of Operations (SBI*net* Enabled)" Version 2.0, June 25, 2008.

[2] U.S. Department of Homeland Security, "Secure Border Initiative C3I Common Operating Picture (COP) Training Manual," Customs and Border Protection, June 2010, FOR OFFICIAL USE ONLY

[3] U.S. Department of Homeland Security, Attachment to (b) (7)(E) (b) (7)(E)

[4] U.S. Department of Homeland Security, "Secure Border Initiative Integrated CONOPS and Requirements Specification," Version 2.1, Customs and Border Protection, July 2007.

[5] Telephonics Corp., "Operator and Basic Maintenance Manual, (b) (7)(E) (b) (7)(E).

[6] National Border Patrol Strategy, Office of Border Patrol, September 2004; (b) (7)(E)

[7] U.S. Department of Homeland Security, "SBI*net* Block I After Action Report with Lessons Learned" Draft Working Version 10, 18 July 2011

[8] U.S. Army Evaluation Center, ATEC, "SBI*net* Block 1, Emerging Results, Emerging Results Brief," 2 March 2011, FOR OFFICIAL USE ONLY

[9] JHU/APL, "Key Points from Capabilities and Limitations Workshop," April 2011.

This Page Intentionally Blank

7. GLOSSARY

Brightness – Adjusting the brightness is typically done to bring out details in the dark portions of the image. (b) (7)(E)

Camera Control – Provides (b) (7)(E)

Classify[1] – To determine the level of threat or intent of the Entity/IoI.

Clutter – Refers to echoes returned from targets that are not important (b) (7)(E)

Communication and Interoperability – Operational functions that address the system's ability to send and receive data.

Configuration – Operational functions that reflect fundamental expectations of the system, and the user's ability to change basic system features. Support the system setup and information security.

Data Management – Operational functions that identify how the data will be utilized, manipulated, and stored by the system.

Detect[1] – To have a method of efficiently discovering the existence of threats on the border.

Deter[1] **–** If potential illegal migrants perceive that any attempt at illegal entry will fail and will result in a penalty, they are less likely to attempt such an entry.

Digital Zoom – Provides the ability to view (b) (7)(images closer. Digital zoom ranges from (b) (7)(E).

Digital Terrain Elevation Data (DTED) – A standard of digital datasets which consist of a matrix of terrain elevation values. Supports many applications, including LOS analyses, terrain profiling, 3-D terrain visualization, mission planning/rehearsal, and modeling and simulation.

Gain – Allows the user to adjust how the optical image formed on the sensor array is converted to an electrical signal. (b) (7)(E)

Foundational Operational Capability (FOC) – Defined in CBP's Measures of Impact (MOI) as Impedance & Denial; Operational Access, Mobility & Rapid Response; Visibility &

[1] U.S. Department of Homeland Security, "Draft CBP Concept of Operations (SBI*net* Enabled)," Version 2.0, June 25, 2008.

Surveillance; Command, Control, Communications, Coordination & Intelligence; and Security Partnerships.

Field of View (FOV) – The area over which the camera sees. (b) (7)(E) (b) (7)(E)

Frequency – (b) (7)(E) is the number of occurrences of a repeating event per unit time.

Item of Interest (IoI)[2] – A detected object or person within the field of operation of possible interest to CBP. Items of Interest may include, but are not limited to, CBP assets and resources that have not yet been identified as such, (b) (7)(E) (b) (7)(E)

Identify[1] – To determine whether an Entity/IoI is a (b) (7)(E).

Image Polarity (b) (7)(E)) – (b) (7)(E images are presented as [redacted] There are two options available, (b) (7)(E)

Image Stabilization – Provides the ability to improve video quality that may become degraded (b) (7)(E).

Limited – Provides some portion of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.

Line of Sight (LOS) – An unobstructed path between sending and receiving devices.

Metadata {video}[3] – is defined by the C3I SRS requirement (b) (7)(E), (b) (7)(E)

Microwave – Frequency waves with wavelengths ranging from as long as one meter to as short as one millimeter, or equivalently, with frequencies between 300 MHz (0.3 GHz) and 300 GHz.

Minimal – Provides basic elements of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.

Mission Elements – Predict, Deter, Detect, Identify, Classify, Track, Respond, Resolve.

Operator Interface – Operational functions that provide an operator friendly COP system.

[2] SBI*net* Glossary, 04/28/2008.
[3] Definitions are from the DHS lexicon.

Predict[1] – To anticipate item of interest (Entity/IoI) actions prior to illegal activity.

Radar Pre-Set – (b) (7)(E) (b) (7)(E)

Reliability, Maintainability, Availability – Operational functions pertains that impact the ability of the system to continuously and effectively operate in all environmental conditions.

[redacted] **Scan Speed** – Most properly defined as the (b) (7)(E)

Respond[1] – To employ the appropriate level of law enforcement resources to successfully address an Entity/IoI.

Resolve[1] – To take final CBP action, criminally, administratively, or otherwise, against an Entity/IoI.

Risk[3] – Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Sector[3] – An operational area of responsibility defined by Office of Border Patrol (OBP).

Significant – Provides a considerable portion of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.

Threat[2] – Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.

Track – To monitor a target or Entity/ IoI by establishing the path of detection within an acceptable level of certainty.

Time to Live (TTL) – The predetermined amount of time an entity is set to stay on the screen. It is defaulted at (b) (7)(E) and can be changed by the operator. Once it is changed, it will reflect the new TTL in minutes.

Time to Expire/"expires" – A countdown timer that starts (b) (7)(E). (b) (7)(E), the "expires" will count down from the time shown in the TTL section displayed on the Reports Portal. (b) (7)(E) when TTL is changed, the Expires counter will begin counting down immediately.

Viewshed – An area of geography that is visible from a fixed LOS vantage point.

Vulnerability[3] – Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

This Page Intentionally Blank

8. ACRONYMS AND ABBREVIATIONS

[redacted] (b) (7)(E)	
AOR	Area of Responsibility
[redacted] (b) (7)(E)	
BP	Border Patrol
[redacted] (b) (7)(E)	
C&L	Capabilities and Limitations
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Coordination, and Intelligence
CBP	Customs and Border Protection
CONOPS	Concept of Operations
COP	Common Operational Picture
COTS	Commercial off-the-shelf
CV	Capability Vignette
DHS	Department of Homeland Security
DTED	Digital Terrain Elevation Data
[redacted] (b) (7)(E)	
FOC	Foundational Operational Capability
FOV	Field of view
GIS	Geographic Information System
[redacted] (b) (7)(E)	
IoI	Item of Interest
[redacted] (b) (7)(E)	
LOS	Line of Sight
[redacted] (b) (7)(E)	
MOI	Measure of Impact
[redacted] (b) (7)(E)	

MTI	Moving Target Indicator
(b) (7)(E)	
NOC	Network Operations Center
OA	Open Architecture
OBP	Office of Border Patrol
OJT	On the Job Training
OTRR	Operational Test Readiness Review
POE	Port of Entry
RF	Radio Frequency
RMA	Reliability, Maintainability, and Availability
RTU	Remote Terminal Unit
(b) (7)(E)	
SBI	Secure Border Initiative
SME	Subject Matter Expert
SOC	Security Operations Center
SWB	Southwest Border
(b) (7)(E)	
(b) (7)(E)	
USBP	United States Border Patrol
VSOC	Visual Security Operations Console

9. ADDITIONAL DOCUMENTS

Key supporting documents are listed below:

Reference Documents			
Item	**Document Number**	**Title**	**Date**
1	D333-000011-1	Requirements Verification and Validation Plan	
2	D333-000017-1	Architecture Description Document	
3	D333-000048	Environments Description Databook (EDD)	
4	D333-000084-1	System Latency Analysis	
5	D333-000094-1	SBI*net* Configuration Management Handbook	
6	D333-000155-1	Configuration Items List	
7	D333-000157-1	C2 Component Qualification Test Detailed Test Plan Vol 1.	9/21/2009
8	D333-000157-2	C2 Component Qualification Test Detailed Test Description Vol. 2	
9	(b) (7)(E)	(b) (7)(E)	
10	(b) (7)(E)	(b) (7)(E) Software Version Description Drawing, version D	7/9/2010
11	(b) (7)(E)	(b) (7)(E) Interface System	
12	(b) (7)(E)	(b) (7)(E) eing C2 STATION SOFTWARE, FOUO, Version	5/27/2010
13	(b) (7)(E)	RTU SOFTWARE INSTALLATION DRAWING, Rev D	7/9/2010
14	(b) (7)(E)	(b) (7)(E) Software Installation Drawing	
15	(b) (7)(E)	(b) (7)(E) Firmware Installation Drawing	8/14/2009
16	(b) (7)(E)	FIRMWARE/SOFTWARE, (b) (7)(E) ,Rev C, FOUO	2/18/2010
17	D333-000247-1	C3I System Tailoring Guide	
18	(b) (7)(E)	(b) (7)(E) System Integration Checkout Procedure	
19	(b) (7)(E)	KIT, PROCESSING (b) (7)(E) FOUO	6/7/2010
20	D333-000299-1	System Design Document (SDD)	
21	D333-000359-1	System Under Test (SUT)	

Reference Documents			
Item	**Document Number**	**Title**	**Date**
22	S333-001001-1	SB*Inet* System of Systems (SoS) A-level Specification	
23	D333-001011-1	Video Data Recording Requirements and Impacts	
24	D333-001015-1	System of Systems A-Level Specification Verification Summary Sheet (VSS) Package	
25	D333-002014-1	SB*Inet* Test and Evaluation Data Management Plan	
26	(b) (7)(E)	Network Logical Architecture, (b) (7)(E)	
27	(b) (7)(E)	(b) (7)(E) FACILITY UPGRADE, (b) (7)(E)_265, RevB	12/10/2009
28	(b) (7)(E)	Tower Site, Communications Relay, (b) (7)(E)_181, (b) (7)(E) Rev E	1/25/2010
29	(b) (7)(E)	TOWER SITE,COMMUNICATION RELAY,(b) (7)(E)_185, (b) (7)(E) Rev E	1/25/2010
30	(b) (7)(E)	TOWER SITE COMMUNICATION RELAY, (b) (7)(E)_187, (b) (7)(E) Rev E	1/25/2010
31	(b) (7)(E)	TOWER SITE,SURVEILLANCE, (b) (7)(E)_287,(b) (7)(E) REV F	1/25/2010
32	(b) (7)(E)	TOWER SITE AND UPGRADE, SURVEILLANCE AND COMMUNICATION RELAY, (b) (7)(E)_032/300,(b) (7)(E) Rev F	1/25/2010
33	(b) (7)(E)	TOWER SITE, SURVEILLANCE, (b) (7)(E)298, (b) (7)(E) , Rev F	1/25/2010
34	(b) (7)(E)	TOWER SITE, SURVEILLANCE, (b) (7)(E)_299, (b) (7)(E) Rev F	1/25/2010
35	(b) (7)(E)	TOWER SITE, SURVEILLANCE, (b) (7)(E)_035, (b) (7)(E) REV F	1/25/2010
36	(b) (7)(E)	TOWER SITE, SURVEILLANCE, (b) (7)(E)_036, (b) (7)(E) REV F	1/25/2010
37	(b) (7)(E)	TOWER SITE, SURVEILLANCE, (b) (7)(E)_290, (b) (7)(E) Rev F	1/25/2010
38	(b) (7)(E)	TOWER SITE, SURVEILLANCE, (b) (7)(E)_041, (b) (7)(E) Rev F	1/25/2010
39	(b) (7)(E)	Tower Site, Surveillance, (b) (7)(E)_085, (b) (7)(E) (b)	1/25/2010
40	(b) (7)(E)	TOWER UPGRADE, COMMUNICATION RELAY, (b) (7)(E)_103, (b) (7)(E) REV E	7/6/2010
41	(b) (7)(E)	TOWER SITE, COMMUNICATION RELAY, (b) (7)(E)_291, (b) (7)(E) Rev E	1/25/2010
42	(b) (7)(E)	(b) (7)(E) Rev A	7/9/2008
43	(b) (7)(E)	Communications Architecture, (b) (7)(E)	

Reference Documents			
Item	**Document Number**	**Title**	**Date**
44	(b) (7)(E)	(b) (7)(E) Network Design for the Southern Border, (b) (7)(E)	
45		(b) (7)(E) Functional Checkout Procedures	11/19/2009
46		(b) (7)(E) System Acceptance Test (SAT) Detailed Test Plan/Procedure Volume 1	
47		(b) (7)(E) System Acceptance Test (SAT) Detailed Test Plan/Procedure Volume 2	
48	S333-200001	Agent Communications System B-2 Specification	
49	(b) (7)(E)	(b) (7)(E) B-2 Specification	
50		INTERFACE CONTROL DOCUMENT (b) (7)(E) [redacted], REV B	8/1/2008
51		(b) (7)(E)	
52		(b) (7)(E)	
53		(b) (7)(E)	
54		(b) (7)(E) Vendor Item Control Drawing	
55		(b) (7)(E) B-2 Specification	
56		(b) (7)(E) B-2 Specification	
57		(b) (7)(E) Item Control Drawing	
58		(b) (7)(E) Vendor Item Control Drawing	
59		(b) (7)(E)	
60	D333-400007-1	INTERFACE CONTROL DOCUMENT Microwave Digital Back-Haul	
61	(b) (7)(E)	Tower (b) (7)(E) B2 Specification	
62		(b) (7)(E)	
63		Interface Requirements Specification (b) (7)(E) (b) (7)(E)	
64		(b) (7)(E) Design Trade Study	
65		Advanced (b) (7)(E) Drawing	
66		Tower (b) (7)(E) Software Requirements Specification	

Reference Documents			
Item	**Document Number**	**Title**	**Date**
67	(b) (7)(E)	SOFTWARE DESIGN DOCUMENT Release 2.0 (b) (7)(E)	
68		(b) (7)(E) User Manual	
69		(b) (7)(E) B-2 Specification	
70		(b) (7)(E)	
71		(b) (7)(E)	
72		(b) (7)(E)	
73		(b) (7)(E) Package	
74	S333-414001	Command and Control Requirements B-2 Specification	
75	(b) (7)(E)	Release 0.5 C2I Software Requirements Specification (b) (7)(E)	
76		INTERFACE REQUIREMENTS SPECIFICATION Release 0.5 C2I Interface Requirements Specification (b) (7)(E)	
77		INTERFACE CONTROL DOCUMENT Release 0.5 C2I Interface Control Document (b) (7)(E)	2/23/2010
78		INTERFACE CONTROL DOCUMENT Network Operations Center (b) (7)(E))/Security Operations Center (b) (7)(E)) CDRL #F055	4/24/2009
79		SOFTWARE VERSION DESCRIPTION, (b) (7)(E) [redacted]	
80		SOFTWARE VERSION DESCRIPTION, Release (b) (7)(E)	3/3/2010
81		Software Version Description Release 2.0(b) (7)(E) [redacted]	
82	D333-414018-1	Release 0.5 Infrastructure Plan – Command, Control and Intelligence (C2I) Facilities	
83	(b) (7)(E)	(b) (7)(E) User Manual	
84		INTERFACE DESIGN DESCRIPTION Release 0.5 Interface Design Descriptions (b) (7)(E)	4/25/2010
85	D333-414024	SBInet C3I COP 0.5 Design Review	2/19 &2/20, 2008
86	(b) (7)(E)	Release 0.5 Software Test Plan/Procedure/Descriptions, Volume 1, (b) (7)(E)	
87	SVD333-414023	C3I COP Release 0.5 Spiral Software Version	

Reference Documents			
Item	**Document Number**	**Title**	**Date**
		Description	
88	D333-414026-1	Release 0.5 Software Test Plan/Procedure/Descriptions, Vol. 1	
89	D333-414026-2	Release 0.5 Software Test Plan/Procedure/Descriptions, Vol. 2	
90	(b) (7)(E)	(b) (7)(E) (b) (7)(E) (b) (7)(E)	10/22/2009
91		BOEING, TERMINAL RACK, (b) (7)(E)	2/27/2009
92	D333-414077-1	Command, Control, Communications and Intelligence Common Operating Picture Software Formal Qualification Test Configuration	
93	(b) (7)(E)	BOEING FACILITY, (b) (7)(E)	3/24/2009
94		BOEING, GOVERNMENT FACILITY INTERFACE CONTROL DRAWING, (b) (7)(E), REV A	10/2/2009
95		WORKSTATION, (b) (7)(E), REV A	3/2/2009
96	S333-417001	Network B-2 Specification, Revision C	10/27/2009
97	[redacted]	Network [redacted] Package	
98	(b) (7)(E)	NETWORK COMPONENT OPERATING SYSTEM SOFTWARE INSTALLATION, REV G	7/1/2010
99	[redacted]	[redacted] Systems and Upgrades, B-2 Specification	
100	D333-504009-1	Interface Control Document Low Speed Wireless	
101	(b) (7)(E)	(b) (7)(E) Surveillance System B-2 Specification	
102		(b) (7)(E)	
103		(b) (7)(E) Tower Shelter	
104		(b) (7)(E)	
105		(b) (7)(E) Tower	
106		(b) (7)(E) Shelter ICD	
107	333-606020	20-DAY LOW-POWER POWER SYSTEMS, REV B	11/27/2007
108	(b) (7)(E)	(b) (7)(E) Power System	
109	333-750000	Information Technology Infrastructure (ITI) Software, REV E	7/9/2010
110	(b) (7)(E)	SBI*net* Technical Report (b) (7)(E) System Acceptance Test (SAT) Workarounds	7/9/2010
111	SBI-TR-326	Block I Geographical Area Laydown Drawing	
112	(b) (7)(E)	(b) (7)(E) Alignment Procedure	

Reference Documents			
Item	**Document Number**	**Title**	**Date**
113		Boeing PowerPoint Presentation, (b) (7)(E) Laydown, FOUO	4/9/2008
114		Adapted from Boeing PowerPoint (b) (7)(E)	2/20/2008
115		CBP PowerPoint Presentation, "Gen 3 AoA Foundational Operational Capabilities"	7/29/2010
116		CBP "Lesson 1.2: COP Monitor - Instructor Guide"	6/1/2010
117		CBP "Web Training (WBT) SBI Concepts Review" FOUO	6/1/2010
118		Boeing "Secure Border Initiative SBI*net* Program Release 0.5 (v0.5.3.2.1) User's Guide Station COP	10/22/2008
119	TRAEN Code: (b) (7)(E)	C3I Common Operating Picture (COP) Instructor-led Training (ILT) Train-The-Trainer, Instructor Guide	6/1/2010
120	TRAEN Code: (b) (7)(E)	C3I Common Operating Picture (COP) Instructor-led Training (ILT) Student Guide	
121		SBI*net* C3I Common Operating Picture (COP) Training, PowerPoint Presentation	6/1/2010
122	No Official Document Number	Release 0.5 (v0.5.3.2.1) User's Guide (Station COP) CDRL # F105	10/22/2008
123		Technical Readiness Review SAT	7/7/2010

Appendix A. FOUNDATIONAL OPERATIONAL CAPABILITIES, MISSION ELEMENTS, AND OPERATIONAL FUNCTIONS DEFINITIONS

The following section provides the definitions and background for the USBP foundational operational capabilities (FOCs), mission elements, and the operational functions used to assess the SBI*net* Block 1 system.

A.1 FOUNDATIONAL OPERATIONAL CAPABILITIES

The leadership at USBP, through an iterative process has defined their agency's Foundational Operational Capabilities necessary to effectively execute the mission of protecting and securing the borders of the United States outside of the port of entries. The USBP definitions of the Generation 3 Analysis of Alternatives Foundational Operational Capabilities (also referred to as Measures of Impact) are provided below[1,2]:

- **Impedance and Denial –** The capability to impede border incursions and deny the threat's use of terrain for advantage in conducting illegal activity and acts of terrorism. This includes the ability to deploy both temporary and persistent impedance/denial solutions in depth throughout the border area.
- **Operational Access, Mobility and Rapid Response –** The capability to gain and maintain access to USBP areas of responsibility (AORs) required for providing security–in–depth along the border area. This includes the ability to rapidly move USBP resources (24/7/365) in (b) (7)(E) terrain, vegetation, and light conditions. This capability also provides USBP with the ability to plan, conduct, and exploit the conduct of special operations to anticipate risks to national security, adapt to emergent threats, and rapidly interdict border incursions of national consequence. This capability also includes the "pooling" and pre–staging of advanced technologies and other USBP resources to surge for emergent operational needs.
- **Visibility and Surveillance –** The capabilities to detect, identify, classify and track all border incursions (24/7/365) in (b) (7)(E), terrain, vegetation, and light conditions.
- **Command, Control, Communications, Coordination, and Intelligence (C4I) –** The capability to effectively and efficiently conduct C4I during the conduct of USBP and joint, interagency, intergovernmental, and multinational (JIIM) operations. This includes deploying and sustaining C4I capabilities required for the full range of security operations (ROSO – national security, law enforcement, emergency response, stability and support ops). This capability must also address unique land, air and maritime C4I capabilities required in urban, rural, and remote areas found in the demanding operational environments of the diverse border regions. This must be a capability (24/7/365 in all

[1] Email communication from CBP/OTIA OID, September 17, 2010, PCR Open Paper 091410.
[2] Email communication from USBP, June 17, 2011, Definitions – Measures of Impact (MOIs).

(b) (7)(E)) tailored to all operational environments in the border area.

- **Security Partnerships –** This capability harnesses the political, social, economic, information, infrastructure, and technology assets/resources of the border areas to enhance our national security. It provides USBP with a robust ability to create, harness, and sustain regional, state, and local partnerships to: 1) increase situational awareness; and 2) create enduring local partnerships and the community commitment required to set the conditions for enduring border security. It includes the ability to demonstrate sound environmental and social stewardship and allows USBP to partner with all security stakeholders to anticipate threats, shape security outcomes, and maximize its influence and impact in AORs throughout our border regions.

A.2 MISSION ELEMENTS

One of CBP's strategic objectives is to establish and maintain effective control of air, land, and maritime borders with the appropriate mix of infrastructure, technology, and personnel. Objective 1.1 in *CBP's 2009–2014 Strategic Plan*[3] states that CBP must:

> *"Establish and maintain effective control of air, land, and maritime borders through the use of the appropriate mix of infrastructure, technology and personnel. A segment of the border between ports of entry is considered under effective control when CBP can simultaneously and consistently achieve the following:*
>
> *(1) **detect** illegal entries into the United States;*
>
> *(2) **identify** and **classify** these entries to determine the level of threat involved;*
>
> *(3) efficiently and effectively **respond** to these entries; and*
>
> *(4) bring each event to a satisfactory law enforcement **resolution**."*

The following definitions for the mission element were obtained from the CONOPS.[4]

- **Predict –** To anticipate illegal traffic actions prior to illegal activity
- **Deter –** To dissuade illegal cross border activity into and out of the United States by creating and conveying a certainty of immediate interdiction upon entry
- **Detect –** To discover the presence of a possible item of interest (IoI)[5]
- **Track –** To follow the progress/movements of an IoI
- **Indentify –** To determine whether an IoI is (b) (7)(E)
- **Classify –** To determine the level of threat or intent of the IoI
- **Respond –** To dispatch or employ law enforcement resources to address an IoI

[3] (b) (7)(E)

[4] U.S. Department of Homeland Security, "Secure Border Initiative Integrated CONOPS and Requirements Specification," Version 2.1, Customs and Border Protection, July 2007.

[5] IoI (b) (7)(E)

- **Resolve –** To take final CBP action, whether criminally, administratively, or otherwise. This includes capture data, process information, etc.

A.3 SYSTEM OPERATIONAL FUNCTIONS CATERGORIES

In order to evaluate Block 1 from a system perspective, a series of functions and categories were derived based on the operational requirements found in various authoritative CBP documents, as well as from a review of tasks needed to support the mission elements. This review yielded the major categories, listed below, from which subcategories were derived to provide a more detailed system examination breakdown.

- Configuration – This pertains to functions that reflect fundamental expectations of the system and other basic system features. Configurations can have implications into operator safety, information assurance, data security, operator access to data, and other basic system features. The high-level configuration functions examined herein are:
  - Configurable/Definable Functionality Set by System Administrator
  - Information Assurance at Multiple Layers
  - Data Security
- Communication and Interoperability – This pertains to functions that address the ability to send and receive data. The topics cover the means for transferring data as well as the types of data that are needed for system operation. Examples of high-level communication and interoperability functions include:
  - Receive and Process Raw Data
  - Send and Receive Data from CBP Agents
  - Send and Receive Data from non-CBP Assets
  - "Plug and Play" Functionality (OA)
- Data Management – This pertains to functions that identify how data will be utilized, manipulated, and stored by the system. The topics cover processing, fusing, manipulating, and storing data. Examples of high-level data management functions include:
  - Fuse Information
  - Prioritize Response to Contact
  - Agent Safety
  - Reporting
  - Store and Retrieve Data
  - Operator/Agent Training
- Operator Interface – This pertains to functions that provide an operator friendly COP system. The topics cover the Graphical User Interface and human systems integration

(HSI) characteristics of the system. Examples of high-level operator interface functions include:

- User Friendliness
- Geographic Based Display
- User Configurable/Definable Functionality
- Icon Display
- Display Identity of Contacts and IoIs (b) (7)(E)
- Display Threat Classification
- Display Track History
- Support Lost Contact
- Predict Location/Area of Uncertainty
- Create Overlays for Search Areas, (b) (7)(E)
- Filter Displayed Data

- Reliability, Maintainability, Availability – This pertains to functions that impact the ability of the system to continuously and effectively operate in all environmental conditions. The topics cover system redundancies, graceful degradation, and overall robustness of the system. Examples of high-level RMA functions include:
  - System Availability
  - Graceful Degradation
  - Reliable Day/Night Operation
  - Reliable (b) (7)(E) Operation
  - Built–in Test/Alert for Failures/Degraded Performance
  - Preventative Maintenance/Test
  - Minor Repair within Non-technician Operator Capability
  - Repair Times

Appendix B. VIEWSHEDS ((b) (7)(E))

B.1 (b) (7)(E)

(b) (7)(E) viewsheds were calculated using (b) (7)(E) data sets (b) (7)(E). A viewshed of the total AOR and individual viewsheds are shown for each (b) (7)(E) (b) (7)(E) used in the SBI*net* system.

B.1.1 (b) (7)(E) COMBINED VIEWSHED

(b) (7)(E)

B.1.2 (b) (7)(E) Tower Locations and Viewshed Percentages

(b) (7)(E)

B.1.3 (b) (7)(E)

(b) (7)(E)

B.1.4 (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

B.1.5 (b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

B.1.6 (b) (7)(E)

(b) (7)(E)

B.1.7 (b) (7)(E)

(b) (7)(E)

B.1.8 (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

B.1.9 (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

B.1.10 [redacted] (b) (7)(E)

[redacted] (b) (7)(E)

B.1.11 (b) (7)(E)

(b) (7)(E)

B.2 (b) (7)(E)

(b) (7)(E) viewsheds were performed using (b) (7)(E) . A viewshed of the total AOR and individual viewsheds are shown for each (b) (7)(E) (b) (7)(E) used in the SBI*net* system.

(b) (7)(E)

B.2.1 (b) (7)(E) COMBINED VIEWSHED

(b) (7)(E)

B.2.2 (b) (7)(E) LOCATIONS AND VIEWSHED PERCENTAGES

(b) (7)(E)

B.2.3 (b) (7)(E)

(b) (7)(E)

B.2.4 (b) (7)(E)

(b) (7)(E)

B.2.5 [redacted] (b) (7)(E)

[redacted] (b) (7)(E)

B.2.6 (b) (7)(E)

(b) (7)(E)

B.2.7 (b) (7)(E)

(b) (7)(E)

B.2.8 (b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

This Page Intentionally Blank

Appendix C. CAPABILITY VIGNETTES

The Capability Vignette (CV) assessment is based on Capability Vignettes developed in the Secure Border Initiative Integrated Concept of Operations (CONOPS) and Requirements Specification.[1] These CVs were developed to describe each capability by illustrating a series of linked activities relevant to the SBI*net* user community and its mission. The CVs provide a source of assessment and context for the system requirements. They provide context for the various ways services and functional activities enable users to complete their mission. The CVs provide another source of assessment from the user perspective, and provides context into the various ways the services and functional activities will enable users to complete their mission. The CVs developed in the SBI CONOPS and Requirements Specification document are intended to allow operational users to understand how a capability will be performed using SBI*net* and trainers to develop training material relevant to the CBP capabilities that need to be performed.

Each CV has several parts:

1. Operational Scenario Synopsis – summarizes the overarching objectives.
2. Activities (functions) – describes specific functions to be performed by the system.
3. Activity description – defines the activity/function it is associated with. This capability assessment is conducted at a system level. The terms used are qualitative in nature and represent the opinions of the component subject matter experts (SMEs).

The assessment of the CBP CONOPS CVs included in this appendix is intended to qualitatively evaluate capabilities that exist within the current SBI*net* Common Operating Picture (COP). Seven of the nine CBP CONOPS CVs are included in the assessment (the two remaining CVs are for capabilities deployed at the ports of entry and outside the scope of the evaluation related to the SBI*net* system). The qualitative designations used to characterize each Capability Vignette are based on SME input and information gained through feedback from operators. As earlier in the document, the table below depicts the legend and qualitative descriptors used in the Capability Vignette assessment.

[1] U.S. Department of Homeland Security, “Secure Border Initiative Integrated CONOPS and Requirements Specification,” Version 2.1, Customs and Border Protection, July 2007.

Block 1 USBP Strategic Planning, Mission Elements, and Tactical Functions Rankings

System and Subcomponent
Significant Provides a considerable portion of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.
Limited Provides some portion of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.
Minimal Provides basic elements of the resources (e.g., forces, equipment, and information) that are needed to achieve the operational capability.
None

Table C–1: Vignette #1 – Detect and View Entity/IoI

Vignette #1 – Detect and View Entity/IoI		
Operational Scenario Synopsis: The user detects an Entity/IoI via sensory data and/or human perception. Once the detection data is received, the user is able to view the data on the COP. The user can collect details of the Entity/IoI via control equipment. The user can then communicate with other users via two-way method communication devices.		
Activity (Function)	**Activity Description from SBI*net* CONOPS**	**Capability Assessment**

(b) (7)(E)

Vignette #1 – Detect and View Entity/IoI		
Operational Scenario Synopsis: The user detects an Entity/IoI via sensory data and/or human perception. Once the detection data is received, the user is able to view the data on the COP. The user can collect details of the Entity/IoI via control equipment. The user can then communicate with other users via two-way method communication devices.		
Activity (Function)	**Activity Description from SBI*net* CONOPS**	**Capability Assessment**

[redacted]

(b) (7)(E)

Table C–2: Vignette #4 – Conduct Primary Processing

Vignette #4 – Conduct Primary Processing		
Operational Scenario Synopsis: Provides the capability for CBP users to first view the Common Operating Picture of a situation or event, and then invite one or more other government agencies to view the same Common Operating Picture in order to facilitate information sharing during a coordinated response.		
Activity (Function)	Activity Description from SBI*net* CONOPS	Capability Assessment

(b) (7)(E)

Table C–3: Vignette #5 – Review and Respond to (b) (7)(E) Data

Vignette #5 – Review and Respond to Intelligence Data		
Operational Scenario Synopsis: The user receive (b) (7)(E) data from different sources and is able to disseminate (b) (7)(E) data that would be valuable for other.		
Activity (Function)	Activity Description	Capability Assessment
(b) (7)(E)		

Table C–4: Vignette #6 – Respond to an Entity/IoI Detection

Vignette #6 – Respond to an Entity/IoI Detection		
Operational Scenario Synopsis: Once it is determined that a response is necessary, the user has access to view resource availability based on status and location. The user has the ability to communicate with other coordinating entities including sending recorded event data. With this information, users will be able to determine necessary response and update response details.		
Activity (Function)	Activity Description	Capability Assessment
(b) (7)(E)		

Table C–5: Vignette #7 – Resolve Entity/IoI Threat

Vignette #7 – Resolve Entity/IoI Threat		
Operational Scenario Synopsis: Once an Entity/IoI has been secured, the user has the ability to interview, access, collect, and verify Entity/IoI attributes. If needed, the user may arrest and transport the Entity/IoI to a station or facility. The user has the ability to coordinate judicial proceedings with other agencies. All Entity/IoI information collected will be used to create an enforcement record.		
Activity (Function)	Activity Description	Capability Assessment
(b) (7)(E)		

Table C–6: Vignette #8 – Communicate and Coordinate Event Response

Vignette #8 – Communicate and Coordinate Event Response		
Operational Scenario Synopsis: The user will be able to communicate with internal and external CBP operators in order to coordinate a response. This response is based on threat level classification and available resources. Users and other operators will be able to view response from detection to resolution.		
Activity (Function)	Activity Description	Capability Assessment
(b) (7)(E)		

Table C–7: Vignette #9 – Conduct (b) (7)(E)*

Vignette #9 – Conduct Law Enforcement Technical Collection		
Operational Scenario Synopsis: (b) (7)(E) program's primary mission is detecting the precise location of any threats against the integrity of the U.S. border by terrorists or criminal organizations for interdiction and/or investigative purposes. This program directly supports the CBP priority mission of achieving effective control of the border.		
(b) (7)(E)		

Appendix D. (b) (7)(E)

The SBI*net* (b) (7)(E) s shown in Figure D–1.

(b) (7)(E)

Figure D–1: [redacted] System Interface

D.1 (b) (7)(E) SYSTEM OVERVIEW

[redacted] (b) (7)(E) Since the atmosphere is relatively transparent to [redacted]. [redacted]

In its most basic form, [redacted].

To detect the presence of a target object, the transmitter generates [redacted] (b) (7)(E) [redacted] (b) (7)(E) [redacted]. Th [redacted], where detection processing is performed. The computer continuously monitors the [redacted]

Just like radio stations operating at different frequencies, [redacted] (b) (7)(E) [redacted] he strength of a target's [redacted] (b) (7)(E) [redacted]

The target's range is most commonly determined by [redacted] (b) (7)(E) [redacted]

In order to determine a target's location requires a [redacted] (b) (7)(E) . .

[redacted] (b) (7)(E)

[redacted] (b) (7)(E)

D.2 [redacted] (b) (7)(E) SUBCOMPONENTS AND SPECIFICATIONS

The [redacted] (b) (7)(E) used in Block 1 is the [redacted] (b) (7)(E) from Telephonics Corporation. [redacted] (b) (7)(E)

The [redacted] consists of a [redacted] (b) (7)(E) his is shown below in Figure D–2:

(b) (7)(E)

—— Solid lines – Hardware interfaces

- - - Dashed lines – Software modules

Source: Telephonics Corp., “Operator and Basic Maintenance Manual, (b) (7)(E) (b) (7)(E)

Figure D–2: (b) (7)(E) Block Diagram

Some of the details described in the subsequent sections are based on information from the (b) (7)(E) user’s manual from Telephonics[1]. Additional installation and interfacing information is included in the SBI*net* (b) (7)(E) Interface Control Document.[2]

D.2.1 (b) (7)(E)

(b) (7)(E)

D.2.2 (b) (7)(E)

(b) (7)(E)

[1] (b) (7)(E) “Operator and Basic Maintenance Manual, (b) (7)(E) (b) (7)(E)

Boeing, “(b) (7)(E) Interface Control Document”, SBI*net* Document (b) (7)(E)

(b) (7)(E).

D.2.3 (b) (7)(E)

(b) (7)(E)

D.2.4 PERFORMANCE SPECIFICATIONS

Some major specifications quoted by the manufacturer of the [redacted] are given in Table D–1. (b) (7)(E) The detection performance for various target types is explained more fully in Section D.3.1.

Table D–1: Some (b) (7)(E) Specifications

Parameter	Value
(b) (7)(E)	(b) (7)(E)

D.3 (b) (7)(E) CAPABILITIES AND LIMITATIONS

Factors that impact (b) (7)(E) performance, capabilities and limitations, and the impact on the FOCs are summarized in this section.

D.3.1 (b) (7)(E) PERFORMANCE FACTORS

The capabilities and limitations of the (b) (7)(E) come from three different sources: the design of the (b) (7)(E) itself, the settings chosen by the operator, and the environment being monitored. Factors from these areas impact the primary (b) (7)(E) performance metrics (b) (7)(E)

(b) (7)(E)

D.3.1.1 (b) (7)(E) Design–Based Factors

The SBI*net* system includes an (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

The detection performance of the [redacted] is a (b) (7)(E). The theoretical detection performance of [redacted] based on its parameters, is shown in Figure D–3. (b) (7)(E) (b) (7)(E) are shown as examples. [redacted], regardless of elevation angle. The maximum (b) (7)(E) and the minimum is [redacted] The ranges given here correspond to *Normal* mode, as discussed later.

(b) (7)(E)

Figure D–3: Maximum Detection Ranges for Example Targets
(calculated based on (b) (7)(E) parameters)

The [redacted] also has a (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

The term viewshed is used to refer to the map of areas that can be "seen" (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted].

[3] DHS, Problem Change Request (PCR) Open Paper, 09/14/2010.
[4] Appendix A – PCR SBInt00003494.
[5] Appendix A – PCR SBInt00002805.
[6] Appendix A – PCR SBInt00001731.

D.3.1.2 [redacted] (b) (7)(E)

[redacted] (b) (7)(E)

[redacted] (b) (7)(E)

[redacted] (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

D.3.1.3 Factors Based on (b) (7)(E) Operator Settings

(b) (7)(E) A discussion of all the internal [redacted] settings that are adjustable is beyond the scope of this document. For ease of use and understanding, these have been grouped into four pre–defined parameter sets, any one of which may be chosen by the COP operator.

The (b) (7)(E) operating modes available to the COP operator include (b) (7)(E). Each of these modes maps to specific [redacted] settings that impacts the capabilities and limitations of the (b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted].

(b) (7)(E)

[redacted]

This Page Intentionally Blank

Appendix E. COMMUNICATIONS

The SBI*net* Block 1 system consists of the tower infrastructure, communications links, and the equipment needed to process the sensor data. Figure E–1 shows the communications tower interfaces.

(b) (7)(E)

Source: [redacted]

Figure E–1: Communications Tower Interfaces

The networked towers enable sensor data to be collected, and transmitted for display on the local COP workstations. This section describes the SBI*net* Block 1 system fixed tower network and communications links.

(b) (7)(E)

The SBI*net* [redacted] (b) (7)(E)

There are two types of towers [redacted] (b) (7)(E) included in the SBI*net* Block–1 deployment. [redacted] (b) (7)(E)

(b) (7)(E)

[redacted] (b) (7)(E)

[redacted] (b) (7)(E)

[redacted] (b) (7)(E)

Each sensor tower is equipped with several subsystems or sensors which aid in target classification, identification, and detection. The sensor tower subsystems include a (b) (7)(E) [redacted] (b) (7)(E)

E.1.1.1 Block 1 Infrastructure Based Factors

(b) (7)(E)

The capabilities and limitations of the legacy components that are currently being used with the communication system is described below:

- (b) (7)(E)

(b) (7)(E)

This Page Intentionally Blank

Appendix F. (b) (7)(E)

Within the SBI*net* Block 1 system architecture, the camera subsystem (b) (7)(E) represents a sensor package (b) (7)(E). The high-level interface (b) (7)(E) is shown in Figure F–1.

(b) (7)(E)

Figure F–1: (b) (7)(E) High-Level System Interface

F.1 (b) (7)(E) SYSTEM OVERVIEW

The camera subsystem consists of (b) (7)(E).

(b) (7)(E)

(b) (7)(E)

Figure F–2: (a) Snapshot (b) (7)(E)

[1] SBI*net* Operator Training, Lesson 2.3, June 2010

A number of factors influence the ability of an operator to detect and recognize objects within the field of view of the cameras. To better understand these factors, consider the simplified model of an imaging system in Figure F–3 below:

(b) (7)(E)

Source: “Target Acquisition,” Lombardo Technical Services (2003.)

Figure F–3: Simple View of a Camera System, from Target to Operator

(b) (7)(E)

The COP operator has control over the functions shown in Table F–1, which correspond to the COP interface shown in Figure H–18: Sensor Management Control Console.

Table F–1: Camera Controls Available to COP Operator

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

- *Focus* – allows the user to sharpen the image collected by adjusting the position(s) of the optics. Typically, focus would need to be adjusted when going from looking at something very near to looking at something far away and vice versa. Figure F–5 is an example of a badly focused image and a well–focused image. (b) (7)(E)

(b) (7)(E)

Source: JHU/APL, (b) (7)(E) July 01, 2009

Figure F–5: Example of a Poorly Focused (bottom) and Well–Focused (top) Image

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

F.2 (b) (7)(E) SYSTEM SUBCOMPONENTS AND SPECIFICATIONS

The optical subsystem at (b) (7)(E) is composed of (b) (7)(E) (b) (7)(E) In addition, the subsystem has (b) (7)(E)

(b) (7)(E)

Source: Derived from SBI*net* Technical Readiness Review, 7/7/2010.

Figure F–8: SBI*net* (b) (7)(E) Components

[3] This is not a representative image from the SBI*net* system; it is used for illustrative purposes only.

For each camera, (b) (7)(E)

The block diagram in Figure F–9 represents the data flow paths at the tower. (b) (7)(E)

(b) (7)(E)

Source: (b) (7)(E) Interface System.

Figure F–9: Block Diagram of SBI*net* (b) (7)(E) Components

- (b) (7)(E)
- [redacted]
- [redacted]

F.2.1 (b) (7)(E)

(b) (7)(E)

(b) (7)(E) Vendor specifications for the (b) (7)(E) camera are provided in Table F–2

Table F–2: (b) (7 Camera Vendor Specifications

(b) (7)(E)

Source: (b) (7)(E) (2008).

F.2.1.1 (b) (7)(Camera Performance

It should be noted that only (b) (7)(camera performance is examined in terms of object size, (b) (7)(E) (b) (7)(E) Again, the following images are for illustrative purposes only (b) (7)(E)

Table F–3 below indicates the rough number of pixels an object would subtend, as a function of range, for the wide and ultra narrow fields of view of the (b) (7)(E) camera. The vehicle can be considered to be a large vehicle, such as a Humvee.

Table F–3: Number of Pixels Covered by Objects that may be of interest

(b) (7)(E)

Note: X indicates a dimension is less than a pixel.

Example images are shown in Table F–4 below. The wide and narrow fields of view represent the extreme fields of view of the camera. (b) (7)(E) [redacted].

Table F–4: (b) (7 Camera (Wide & Ultra Narrow Field of View)

(b) (7)(E)

[4] DHS, email communication, June–October 2010.

(b) (7)(E)

Source: Images taken from (b) (7)(E)

F.2.1.2 (b) (7)(Camera Performance: Ultra Narrow Field of View

The ultra narrow field of view of the (b) (7)(E) provides useful imagery, in terms of the number of pixels subtended by the target. Table F–5 below shows example imagery. Again, this imagery should be considered ‘the best possible,’ (b) (7)(E) (b) (7)(E)

Table F–5: (b) (7 Camera (Ultra Narrow Field of View)

(b) (7)(E)

Source: (b) (7)(E) [redacted]

F.2.2 (b) (7)(E) CAMERA

Vendor specifications for the (b) (7)(E) camera are provided in Table F–6.

Table F–6: (b) (7)(E) Camera Vendor Specifications

(b) (7)(E)

(b) (7)(E)

F.2.3 (b) (7)(E)

The (b) (7)(E) deployed at (b) (7)(E) is the (b) (7)(E) Additional product specifications are provided in Table F–7.

Table F–7: (b) (7)(E) Vendor Specifications

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Figure F–10: (b) (7)(E)

(b) (7)(E)

F.2.4 (b) (7)(E)

Vendor specifications for the (b) (7)(E) are provided in Table F–9.

Table F–9: (b) (7)(E) Vendor Specifications

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

F.2.5 (b) (7)(E)

(b) (7)(E)

(b) (7)(E) A diagram of the process is provided in F.2.5.

[5] DHS, personal communication, June–October 2010

(b) (7)(E) can be used to effectively take out [redacted] appearing, this is shown below in Figure F–11

(b) (7)(E)

The camera captures a series of events, however (b) (7)(E) the content of each frame is offset with respect to the next, as show in the top row of Figure F–11. (b) (7)(E) stitches together the contents of sequential frames so as to keep the [redacted] (b) (7)(E) as shown in the lower row of Figure F–11. The result of which is that, [redacted]

In addition, if the [redacted] *is based on processing multiple frames, the* [redacted] An example would be p (b) (7)(E)

F.2.6 (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Appendix G. (b) (7)(E)

(b) (7)(E)

.

(b) (7)(E)

(b) (7)(E)

Figure G–1: (b) (7)(E) High-Level System Interface

G.1 (b) (7)(E) SYSTEM OVERVIEW

(b) (7)(E) systems deployed for border security contain a (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

G.2 (b) (7)(E) SUBCOMPONENTS AND SPECIFICATIONS

The following section provides details of the (b) (7)(E) system and the legacy (b) (7)(E) (b) (7)(E)

G.2.1 (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Source: SBI*net* System Design Document (SDD), (b) (7)(E), November 24, 2009, Figure 2–19.

Figure G–2: (b) (7)(E) **Communication Architecture**

(b) (7)(E) The (b) (7)(E) system is shown in Figure G–3.

(b) (7)(E)

The interface with the COP has been implemented as planned; (b) (7)(E)

(b) (7)(E)

G.2.2 (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Operator feedback indicated that:

(b) (7)(E)

G.2.3 (b) (7)(E) Performance Factors

Factors that impact (b) (7)(E) performance include (b) (7)(E)

(b) (7)(E)

[25] DHS, Problem Change Request (PCR) Open Paper, 09/14/2010

[26] Appendix A – SBInt00003337

Appendix H. COMMON OPERATIONAL PICTURE (COP)

(b) (7)(E) COP communicates with the (b) (7)(E) directly to retrieve data from the sensor feeds, and to display that information on [redacted] that comprise the COP workstation (see Figure H–1). Operators and managers use the COP to maintain situational awareness in their respective area of responsibility. This section describes the COP workstation and documents its capabilities and limitations.

(b) (7)(E)

Figure H–1: COP High-Level System Interface

H.1 COP SYSTEM OVERVIEW

The COP functions as a common display of shared information and is best suited to provide enhanced and consolidated situational awareness at the operational level, although it may also be employed tactically at the sector level. The COP supports sector field operations primarily in resource allocation efforts.

Basic COP capabilities and functionalities are incorporated into the displays that are presented to the operators. Actions by the operator are generally a result of training, experience, and cues that are purposefully presented to the operator by the COP.

H.2 COP OPERATION AND SPECIFICATIONS

The COP is located in a secure facility. COP operators (b) (7)(E)

The COP Workstation consists of (b) (7)(E)

(b) (7)(E)

Source: CBP "Web–based Training (WBT) SBI Concepts Review," June 2010, FOUO.

Figure H–2: COP Workstation

To use the COP system, users must [redacted] (b) (7)(E)

H.2.1 COP MONITOR

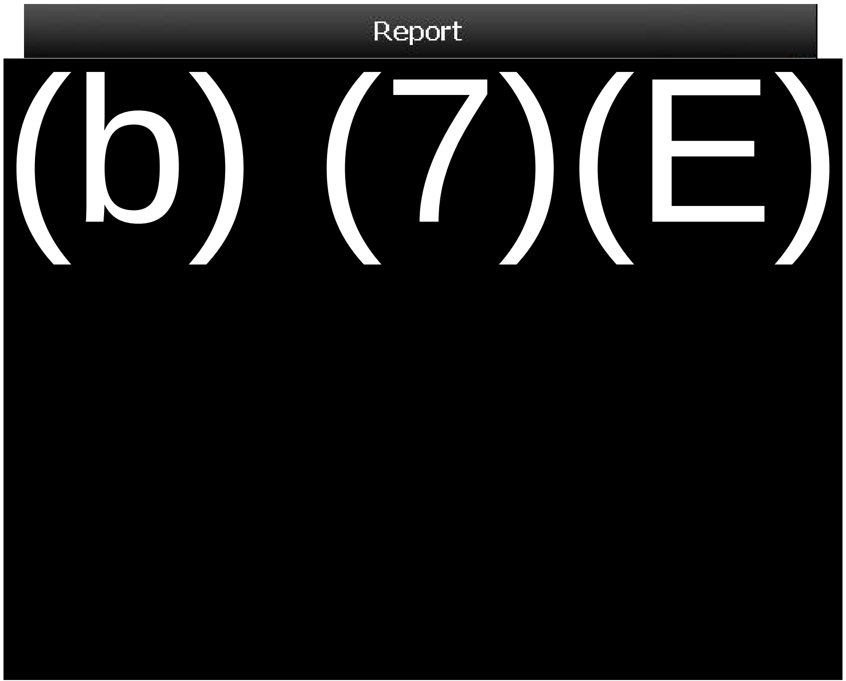
The display for the COP is [redacted] (b) (7)(E)

[redacted] (b) (7)(E)

Source: CBP "Lesson 1.2: COP Monitor – Instructor Guide", June 2010.

Figure H–3: COP Monitor Display

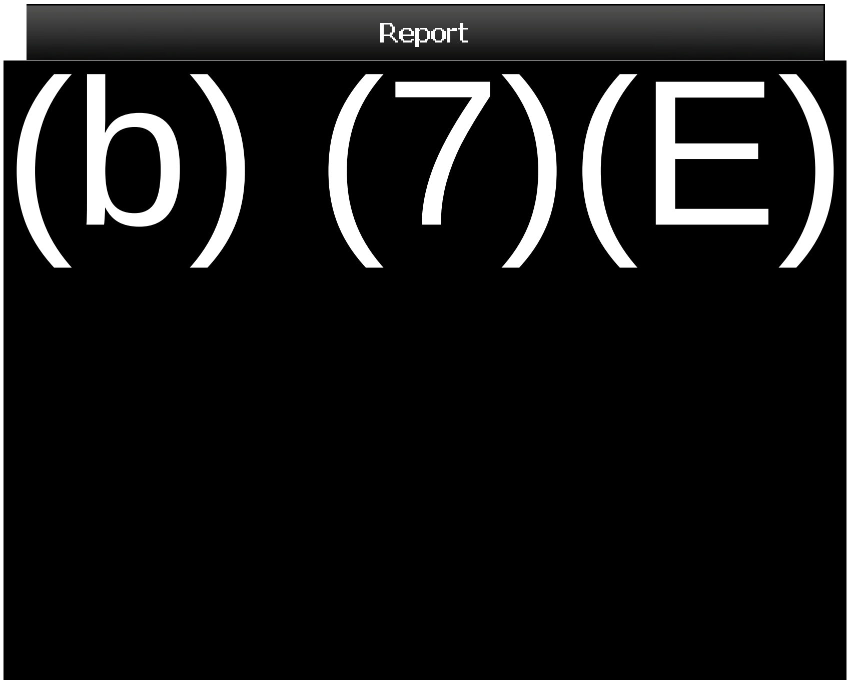
(b) (7)(E)



(b) (7)(E)

Source: CBP "Lesson 1.2: COP Monitor – Instructor Guide", June 2010.

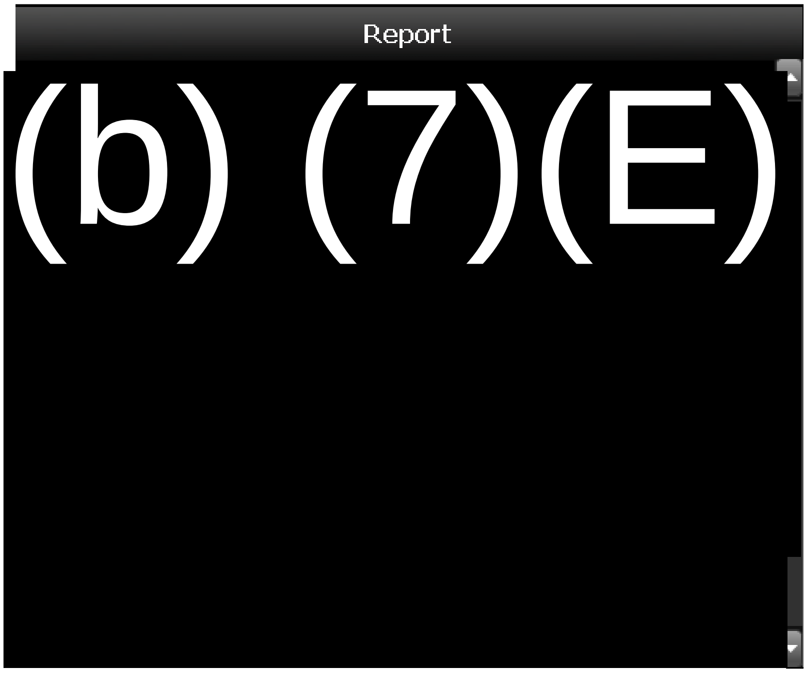
Figure H–5: Report Tower Selected – (b) (7)(E)



(b) (7)(E)

Source: CBP "Lesson 1.2: COP Monitor – Instructor Guide", June 2010.

Figure H–6: Report Agent Selected – (b) (7)(E)

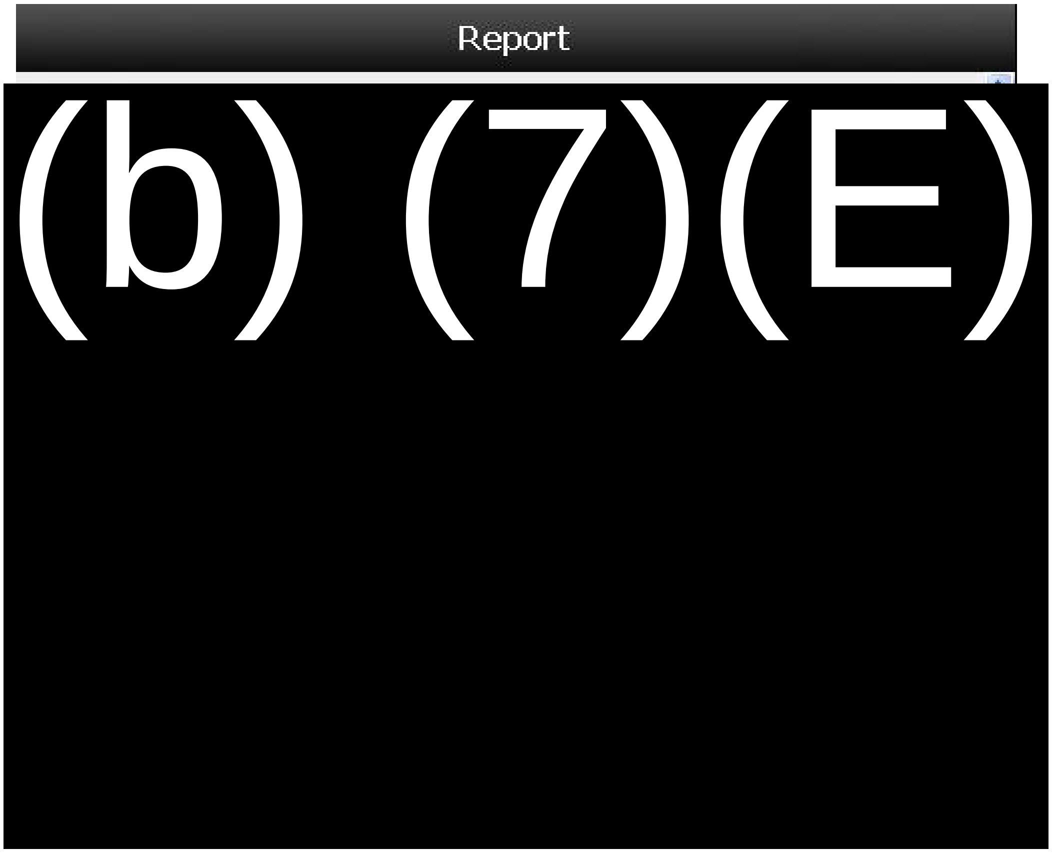


(b) (7)(E)

Source: CBP “Lesson 1.2: COP Monitor – Instructor Guide”, June 2010.

Figure H–7: Report Entity Sighting Selected – (b) (7)(E)

(b) (7)(E)



(b) (7)(E)

Source: Boeing "Secure Border Initiative SBI*net* Program Release 0.5 (v0.5.3.2.1) User's Guide (Station COP), 10/22/2008.

Figure H–8: Report Display Mouse Right Click Options

Alerts Display – (b) (7)(E)

The purpose of the Alerts Display is to communicate information throughout the system to other COP operators (b) (7)(E)

(b) (7)(E).

(b) (7)(E)

Source: CBP "Lesson 1.2: COP Monitor – Instructor Guide", June 2010.

Figure H–9: Alerts Display

Chat Portal – ***This portal allows operators who are logged into the*** (b) (7)(E) ***Figure H–10).*** (b) (7)(E)

(b) (7)(E)

Source: CBP "Lesson 1.2: COP Monitor – Instructor Guide", June 2010.

Figure H–10: Chat Portal

(b) (7)(E)

(b) (7)(E)

Source: CBP “Lesson 1.2: COP Monitor – Instructor Guide”, June 2010

Figure H–11: (b) (7)(E)

Tabs – (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Source: CBP “Lesson 1.2: COP Monitor – Instructor Guide”, June 2010

Figure H–12: Tabs

(b) (7)(E)

[27] DHS, Problem Change Request (PCR) Open Paper, 09/14/2010

(b) (7)(E)

(b) (7)(E)

Source: CBP "Lesson 1.2: COP Monitor – Instructor Guide", June 2010

Figure H–13: (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

H.2.3 VRM

The VRM is used primarily for video recording and storage, as well as video playback and retrieval capabilities. In this capacity, the VRM functions similarly to a household VCR/DVR. A representative screenshot is captured and displayed in Figure H–19.

(b) (7)(E)

Source: CBP “Lesson 1.2: COP Monitor – Instructor Guide”, June 2010

Figure H–19: VRM Display

Appendix I. OPEN ARCHITECTURE (OA) PRINCIPLES

The use of proprietary software hinders the ease of software updates, maintenance, and subsequent integration of new components ("plug and play"). Use of /conformation to open architecture (OA) principles can facilitate a "plug and play" environment – easier software updates, maintenance and integration of new components. OA employs the following principles.[1,2]

- Open standards that satisfy the following criteria:
  - Details necessary for interoperable implementation are included
  - Standards are free and publically available
  - Patents essential to implementation are royalty free with unrestricted used
  - Patents will not be asserted when used in open-source software
  - No execution of licensing, non-disclosure, grants, or other restrictions when deploying a conforming implementation of a standard
  - No dependencies on any other technology or standard that fails to meet the above criteria
- Modularity – a set of properties that support independence of operations using the following principles:
  - Partitioning into discrete, scalable, self-contained units of functionality, and well defined, easily understandable module interfaces.
- Interoperability – ability of two or more capabilities to exchange and use information. From a DoD perspective, "the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together."[3] In the context of the CBP COP, it is the ability of COP systems to exchange data, information, and services from other systems and for these systems to effectively operate together. OA facilitates interoperability by 1) requiring the use of data models defined by open standards, 2) requiring the use of common metadata that is discoverable in repositories based on open standards, and 3) requiring the use of open standards-based interfaces between COP systems.
- Extensibility – components are designed so that future capabilities can be added.

[1] Nelson, E.R., *Open Architecture Technical Principles and Guidelines 1.5.8,* International Business Machines Corporation, IBM Federal CTO Office, 30-Sep-2008.

[2] Office of Technology Innovation and Acquisition, "Open Architecture (OA), Common Operating Picture (COP), Standards Guideline Document (SGD), April 2011.

[3] "Interoperability and Supportability," *Defense Acquisition Guidebook*, Defense Acquisition University, U.S. Department of Defense, 24-Sep-2009, (b) (7)(E)

- Reusability – a component may be used in multiple operational contexts, providing similarly capability to each context.
- Composability – components can be recombined and assembled in various combinations to create new capabilities.
- Maintainability – the ease with which the components of a capability may be maintained after installation until end of life.

Appendix J. QUICK REFERENCE GUIDES (QRG)

The quick reference guides (QRGs) supplement the C&Ls, SBI*net* Training, workarounds, tips and hints. They are intended to provide the operator with substantive material in a condensed format, less than two pages. Figure K–1 is a list of the QRG topics.

(b) (7)(E)

Figure J–1: Quick Reference Topics

J.1 COP

(b) (7)(E)

(b) (7)(E)

J.2 (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

J.3 (b) (7)(E) CAMERAS

(b) (7)(E)

(b) (7)(E)

J.4 (b) (7)(E)

(b) (7)(E)

J.5 MISSION ELEMENTS

(b) (7)(E)

This Page Intentionally Blank